Capitulo 3
Instalación y Configuración de Servicios DHCP, DNS y WINS

1. Introducción

Durante este capítulo Usted irá asimilando conocimientos acerca de los servicios de red tales como DHCP (Dynamic Host Configuration Protocol), WINS (Windows Internet Name System) y DNS (Domain Name System). Este último, en particular, le será de mucha utilidad para el desarrollo del capítulo 4.

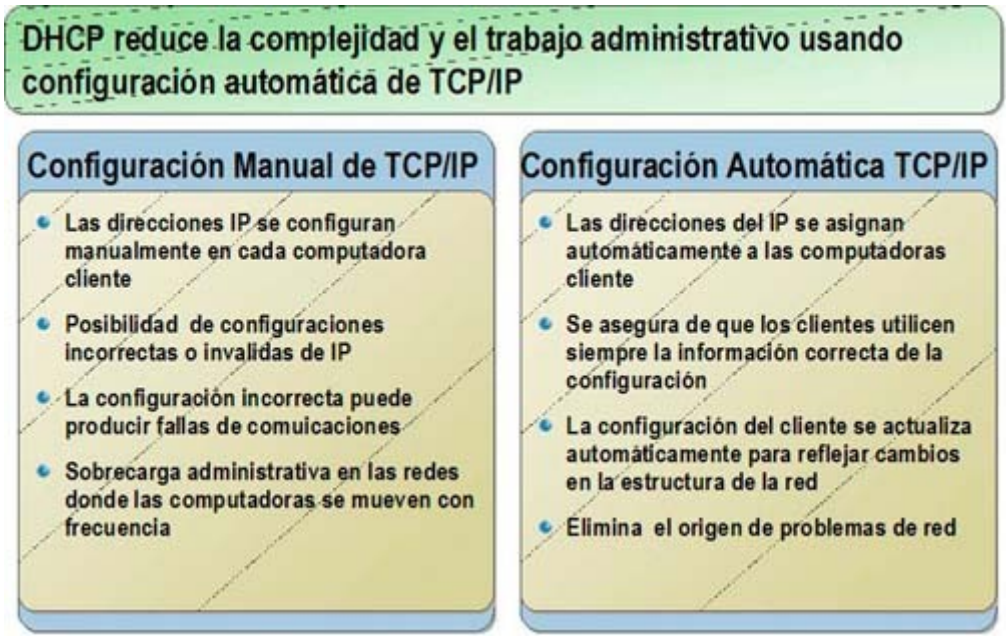
Para la realización de las prácticas contenidas en el presente módulo, necesitará la instalación de Windows Server 2003 que realizó en la práctica 1 del capítulo 2, y una instalación adicional.

Al finalizar este capítulo Usted tendrá la habilidad de:

- Describir las características de los servicios DHCP, DNS y WINS.
- Instalar y configurar servicios de red.
- Solucionar problemas de servicios de red.

2. DHCP - Dynamic Host Configuration Protocol

2.1. ¿Por qué utilizar DHCP?



© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

2.1.1. Definición

Dynamic Host Configuration Protocol (DHCP) es un estándar IP para simplificar la administración de la configuración del IP del cliente. El estándar DHCP permite que Usted utilice los servidores de DHCP para manejar la asignación dinámica de las direcciones y la configuración de otros parámetros IP para clientes DHCP en su red.

2.1.2. ¿Por qué utilizar DHCP?

En redes TCP/IP, DHCP reduce la complejidad y el trabajo administrativo de re-configurar las computadoras cliente.
Para entender por qué DHCP es útil para configurar clientes TCP/IP, es importante comparar la configuración manual de TCP/IP con la configuración automática que utiliza DHCP.

2.1.3. Configuración manual de TCP/IP

Cuando Usted realiza la configuración IP para cada cliente, ingresando manualmente información como la IP address, subnet mask o default gateway, pueden llegar a producirse errores de tipeo, que es probable deriven en problemas de comunicación o problemas asociados a la IP duplicada. Por otra parte, hay carga administrativa adicional en las redes donde las computadoras se mueven con frecuencia de una subnet a otra y, en adición, cuando necesita cambiar un valor IP para varios clientes, tiene que actualizar la configuración IP de cada cliente.

2.1.4. Configuración automática TCP/IP

Cuando Usted configura un DHCP Server para dar soporte a clientes DHCP, éste provee automáticamente la información de la configuración a clientes DHCP y también se asegura que los clientes de la red utilicen la configuración correcta. Además, si Usted necesita realizar un cambio en la configuración IP de varios clientes, podrá realizarlo una vez en el DHCP Server, para que el DCHP actualice automáticamente la configuración del cliente reflejando el cambio.

Ejemplo

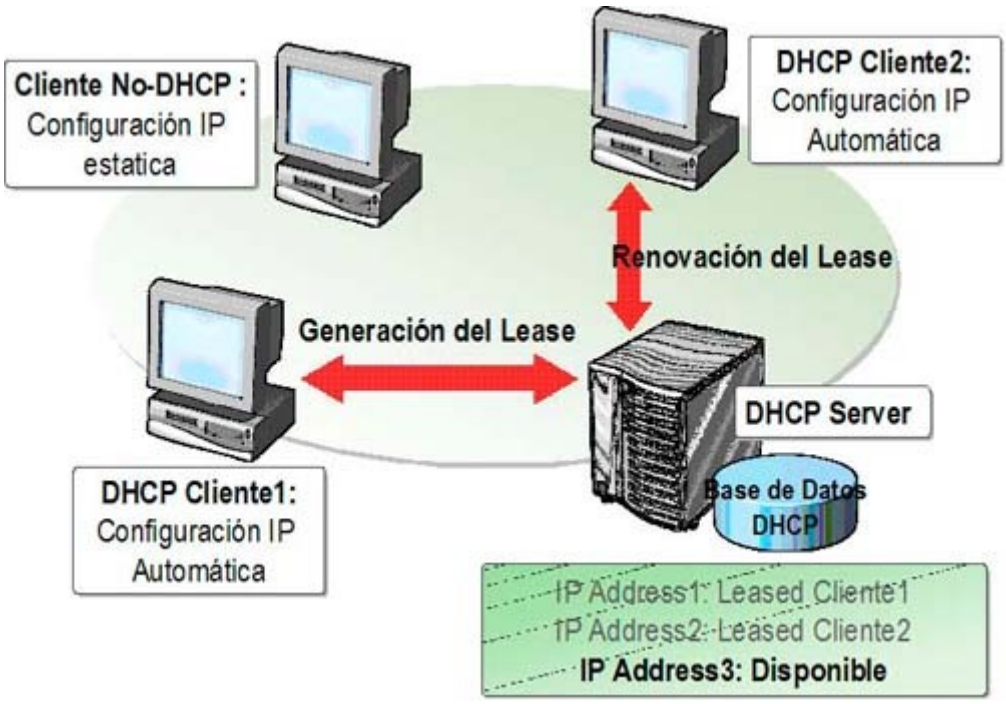
Usted necesita configurar 100 computadoras con la configuración IP, pero sin DHCP no le quedará otra alternativa que configurar manualmente cada una de las computadoras individualmente. A esto hay que sumarle que se tiene que documentar la configuración IP de cada cliente, y que si se tiene que realizar un cambio en la configuración IP de los clientes, también tendría que re-configurarla manualmente en cada uno de ellos.

Pero DHCP tiene la solución a esto. Con DHCP Usted sólo tendrá que agregar la configuración al DHCP Server, que actualiza los 100 clientes de la red. Además, cuando necesite realizar un cambio de configuración IP, el mismo será efectuado una vez solamente en el DHCP Server, requiriendo simplemente que cada cliente TCP/IP renueve su configuración.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.2 ¿Cómo el DHCP asigna direcciones IP?



2.2.2.1 Introducción

DHCP permite manejar la asignación de IP de una localización central, y por lo tanto Usted puede configurar el DHCP Server para asignar direcciones de IP a una sola subnet o múltiples subnets. Asimismo, el DHCP Server puede asignar la configuración IP a los clientes en forma automática.

2.2.2.2 Definición

El ***lease*** es el espacio de tiempo en el cual un cliente DHCP puede utilizar una configuración dinámicamente asignada de IP. Antes de la expiración del tiempo de lease, el cliente debe renovarlo u obtener un nuevo lease del DHCP.

2.2.2.3 Asignación de direcciones IP

El DHCP administra la asignación y el release de la configuración IP, concediendo la configuración IP al cliente. El estado del DHCP lease depende del tiempo en que el cliente pueda utilizar los datos de la configuración IP antes de liberarla y después de renovar los datos. El proceso de asignar la configuración IP se conoce como ***DHCP Lease Generation Process***, y el proceso de renovar los datos de la configuración IP se conoce como ***DHCP Lease Renewal Process***.

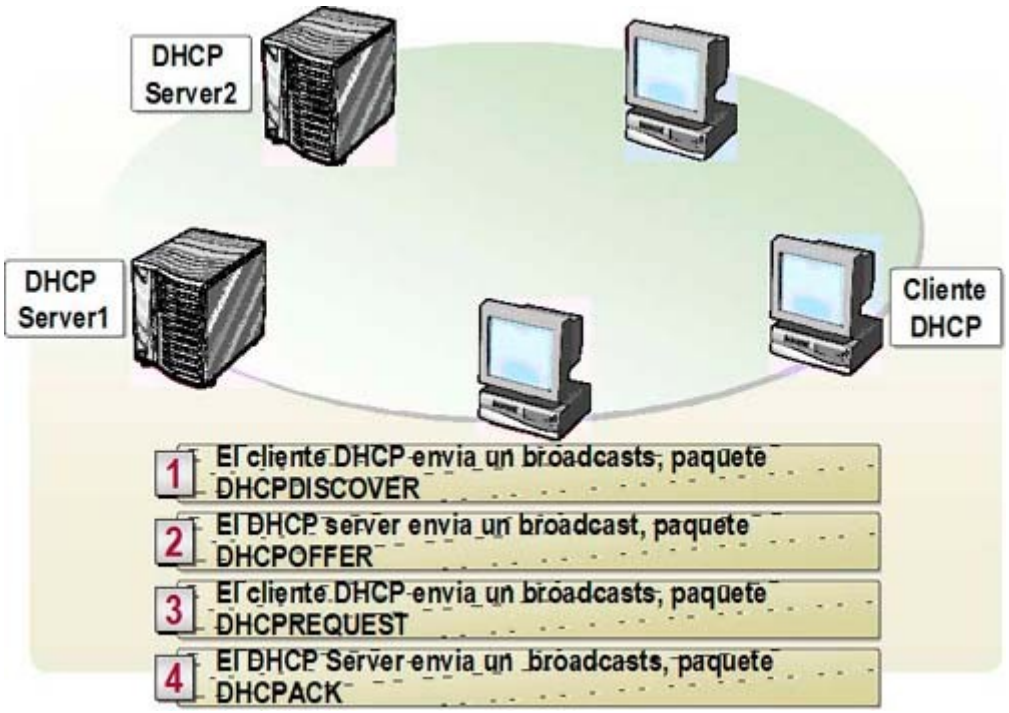
La primera vez que un cliente DHCP se agrega a la red, el mismo debe solicitar la configuración IP al DHCP Server para que, cuando éste reciba la solicitud, el server seleccione una dirección IP del rango de direcciones que el administrador ha definido en el scope. El DHCP Server ofrece la configuración IP al cliente de DHCP. Si el cliente acepta la oferta, el DHCP Server asignará la dirección IP al cliente por un período de tiempo especificado. El cliente entonces utilizará la dirección IP para tener acceso a la red.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

2.3. ¿Cómo funciona el proceso DHCP Lease Generation?



El cliente DHCP envía un broadcasts, paquete DHCPDISCOVER para localizar al DHCP Server. Este paquete DHCPDISCOVER es el mensaje que los clientes DHCP envían la primera vez que se conectan a la red y solicitan la información IP de un DHCP Server. Existen dos formas de comenzar el proceso DHCP Lease Generation. La primera ocurre cuando una computadora cliente se enciende o se inicia TCP/IP por primera vez, y la segunda ocurre cuando un cliente intenta renovar su lease y no lo logra. (Por ejemplo, un cliente puede no lograr una renovación cuando Usted lo mueve a otra subnet.)

El DHCP Server envía un broadcast paquete DHCPOFFER al cliente. El paquete DHCPOFFER es un mensaje que el DHCP Server utiliza para ofrecer el lease de una dirección IP al cliente, cuando éste se conecta a la red. Cada DHCP Server que responde, reserva la dirección IP ofrecida para no ofrecerla nuevamente a otro cliente DHCP, antes de la aceptación del cliente inicial. Si el cliente no recibe una oferta después de cuatro peticiones, utiliza una IP en la gama reservada a partir del 169.254.0.1 a 169.254.255.254. El uso de una de estas direcciones auto-configuradas IP asegura que los clientes situados en una subnet DHCP Server inaccesible, puedan comunicarse con otros clientes. Mientras tanto el cliente DHCP continúa buscando un DHCP Server disponible cada cinco minutos. Cuando el DHCP Server llegue a estar disponible, los clientes recibirán direcciones válidas IP, permitiendo que esos clientes se comuniquen con clientes en su subnet y en otras también.

El cliente DHCP envía un broadcasts, paquete DHCPREQUEST. El paquete DHCPREQUEST es el mensaje que un cliente envía al DHCP Server para solicitar o renovar su lease de IP. El cliente DHCP responde al primer paquete DHCPOFFER que recibe con un broadcasts de DHCPREQUEST para aceptar la oferta. El paquete DHCPREQUEST incluye la identificación del server que oferta y el cliente que aceptó. Todos los otros DHCP Servers después eliminan sus ofertas y conservan sus direcciones de IP para otros lease.

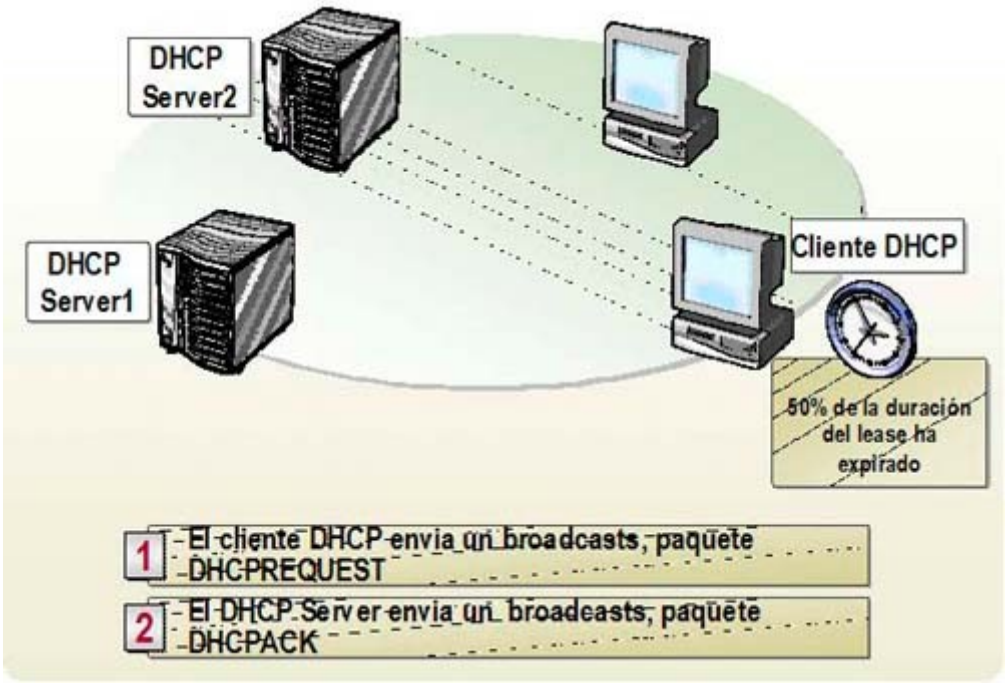
El DHCP server envía un broadcast, DHCPACK al cliente. El paquete DHCPACK es un mensaje que DHCP Server envía a un cliente como acuse de recibo y finalización del proceso de lease. Este mensaje contiene un lease válido para la dirección IP y la otros datos de configuración IP. Cuando el cliente DHCP recibe el acknowledgment, inicia TCP/IP usando la configuración IP provista por el DHCP Server.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Nota: Usted puede ver todo el proceso de lease capturando los paquetes con Network Monitor. Tenga en cuenta que el cliente y el server utilizan los puertos 67 y 68 UDP. Para realizar el proceso en ambientes seguros será necesario que permita la comunicación de esos puertos entre el cliente y el server.

2.4 ¿Cómo funciona el proceso DHCP Lease Renewal?



2.4.1. Definiciones

DHCP Lease Renewal Process es el proceso por el cual un cliente DHCP renueva o actualiza sus datos de configuración IP con el DHCP Server.

El cliente DHCP renueva la configuración IP antes de la expiración del tiempo de lease. Si el período de lease expira y el cliente DHCP todavía no ha renovado su configuración IP, pierde los datos de la configuración IP y comienza nuevamente el proceso DHCP Lease Generation.

2.4.2. Período de Lease

El proceso de Lease Renewal es el resultado del valor de tiempo del lease. El valor de período de lease se asegura que el DHCP mantenga la información IP y que los clientes actualicen o renueven regularmente sus datos de configuración IP. Teniendo DHCP se mantiene esta información e implica que puede administrar el direccionamiento IP desde el DHCP Server. El cliente debe renovar su configuración IP antes de la expiración del período de lease. En los intervalos específicos, un cliente DHCP intenta renovar su lease para asegurarse tener actualizada su configuración. En cualquier momento durante el período de lease, el cliente DHCP puede enviar un paquete de DHCPRELEASE al DHCP Server para liberar la configuración IP y para cancelar el lease restante.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso
Powered by itsitio.com

2.4.3. Proceso automático "Lease Renewal"

Un cliente DHCP intenta renovar automáticamente su lease al 50% del tiempo de expiración. El cliente DHCP también intenta renovar su lease cada vez que la computadora se reinicie, y para intentarlo envía paquete de DHCPREQUEST al DHCP Server directamente, del cual obtuvo el lease. Si el DHCP Server está disponible, renueva el lease y envía al cliente un paquete de DHCPACK con la nueva duración del lease y cualquier parámetro de configuración actualizado. El cliente actualiza su configuración cuando recibe el acknowledgment. Si el DHCP Server no está disponible, el cliente continuará utilizando sus parámetros actuales de configuración. Si el cliente DHCP no puede renovar su lease la primera vez, entonces el cliente DHCP enviará un broadcasts DHCPDISCOVER para actualizar su lease de la dirección cuando expira al 87.5 % de la duración del lease. En esta etapa, el cliente DHCP acepta el lease que cualquier DHCP Server le ofrezca.

Si el cliente DHCP reinicia su computadora y el DHCP Server no responde al paquete DHCPREQUEST, el cliente DHCP intentará conectar con el Default Gateway. Si esta tentativa falla, el cliente cesará el uso de la dirección IP. Si el DHCP Server responde con un paquete DHCPOFFER para actualizar el lease del cliente, éste puede renovar su lease de acuerdo a la oferta del mensaje del server y continúa la operación. Pero si el lease expiró, el cliente deberá suspender inmediatamente el uso de la dirección IP actual. El cliente DHCP, entonces, comenzará un nuevo proceso de DHCP Lease Discovery, intentando obtener un nuevo lease de una nueva IP. Si el cliente DHCP falla al recibir la IP, el cliente se asignará una dirección usando la asignación automática de IP en el rango 169.254.0.0.

2.4.4. Proceso manual Lease Renewal

Si necesita actualizar la configuración DHCP inmediatamente, Usted puede renovar manualmente el lease IP.(Por ejemplo, si quiere que los clientes DHCP obtengan rápidamente la dirección del DHCP Server de un nuevo router instalado en la red, renueve el lease del cliente para actualizar la configuración.)

Ejemplo: c:\inconfig /renew

2.5. Práctica 1: ¿Cómo agregar el servicio DHCP Server?

Para agregar un DHCP Server, Usted deberá instalar DHCP Service en una computadora corriendo Microsoft® Windows® Server 2003.

Antes de agregar el servicio DHCP Server:

- Verificar que la configuración IP en el servidor esté correcta.
- Verificar que la configuración IP del servidor contenga una dirección IP estática y una subset mask en ambientes ruteados un Default Gateway.
- Verificar que la cuenta de usuario tenga los permisos correctos.

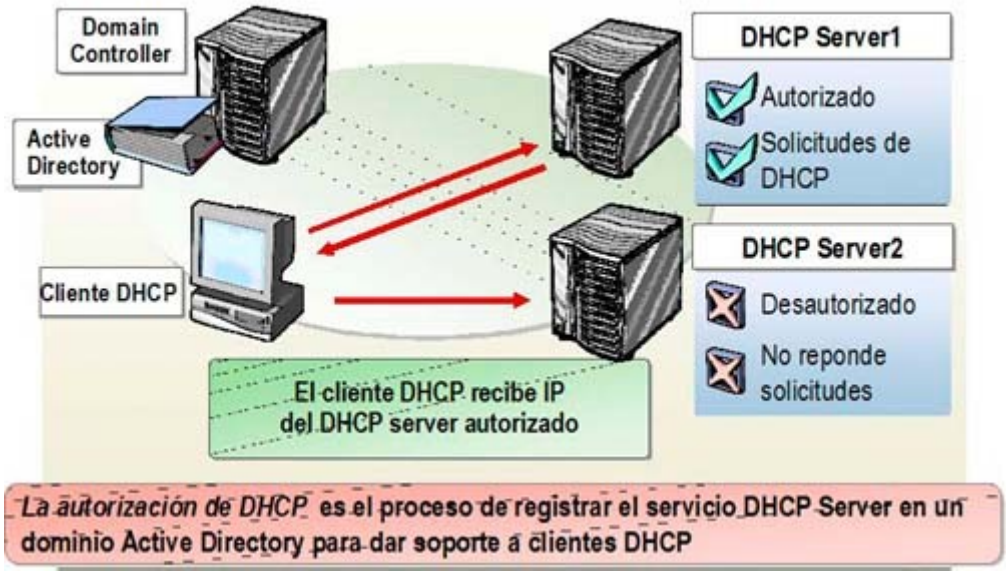
© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Para agregar el servicio DHCP Server deberá:

1. Iniciar sesión usando una cuenta no-administrativa.
2. Hacer click en ***Start*** y después en ***Control Panel***.
3. Abrir las ***Administrative Tools*** en el Control Panel y hacer click derecho en ***Manage Your Server***, seleccionando ***Run as***.
4. Seleccionar ***The following user*** en el cuadro ***Run As*** e ingresar una cuenta de usuario y password que tenga los permisos apropiados para realizar la tarea, haciendo click en ***OK***.
5. Hacer click ***Add or remove a role*** de la ventana Manage Your Server.
6. Hacer click en ***Next*** de la página ***Preliminary Steps***.
7. Seleccionar ***DHCP server*** en el wizard Configure Your Server, y en ***Next***.
8. Hacer click en ***Next*** de la página ***Summary of Selections***,
9. Hacer click en ***Cancel*** del wizard New Scope para no crear el scope en ese momento.
10. Hacer click en ***Finish*** del wizard Configure Your Server.

2.6. ¿Cómo se autoriza el servicio DHCP Server?



2.6.1. Definiciones

La autorización de DHCP es el proceso de registrar el servicio DHCP Server en un dominio Active Directory® Service, con el propósito de dar soporte a clientes DHCP. La autorización DHCP es solo para DHCP Servers corriendo Windows Server 2003 y Windows 2000 en Active Directory.

2.6.2. ¿Por qué autorizar el DHCP Server?

Autorizar al DHCP Server provee la capacidad de controlar la adición de los DHCP Servers al dominio. La autorización debe ocurrir antes que el DHCP Server pueda otorgar leases a clientes DHCP. Solicitar la autorización de DHCP Servers previene que DHCP Servers desautorizados ofrezcan direcciones IP inválidas a clientes.

Si Usted está configurando un DHCP Server, la autorización debe ocurrir como parte del dominio Active Directory. Si Usted no autoriza el DHCP Server en Active Directory, el servicio DHCP no se

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

podrá iniciar correctamente y entonces el DHCP Server no podrá responder a los pedidos de clientes. El DHCP Server controla el direccionamiento IP enviado a los clientes DHCP en la red. Si el DHCP Server se configura incorrectamente, los clientes recibirán una configuración incorrecta de direccionamiento IP.

2.6.3. ¿Por qué un DHCP Server autorizado requiere Active Directory?

Active Directory se requiere para autorizar un DHCP Server. Con Active Directory, los DHCP Servers no autorizados no pueden responder a los pedidos de clientes. El servicio DHCP Server, en un server miembro de Active Directory, verifica su registración con un Domain Controller de Active Directory. Si el DHCP Server no está registrado, el servicio no se iniciará y consecuentemente el DHCP Server no asignará direcciones a clientes.

2.6.4. Stand-alone DHCP Server

Bajo ciertas circunstancias, un DHCP Server corriendo Windows 2000 o Windows Server 2003, se inicia si incluso no está autorizado. Si el DHCP Server corriendo Windows Server 2003 o Windows 2000 está instalado como stand-alone server no es miembro de Active Directory. Y si está situado en una subnet donde DHCPINFORM no será transmitido a otros DHCP Servers autorizados, el servico DHCP Server inicializará y proveerá leases a clientes en la subnet.

Un stand-alone server corriendo Windows 2000 o Windows Server 2003 envía un paquete broadcast DHCPINFORM. Si no hay respuesta al paquete DHCPINFORM, entonces el servicio DHCP Server inicializará y comenzará a atender a los clientes. Si un DHCP Server autorizado recibe un paquete DHCPINFORM, responde con un paquete DHCPACK y entonces el servicio DHCP Server parará. Un stand-alone DCHP Server continuará funcionando si recibe un DHCPACK de otro DHCP Server que no sea miembro de Active Directory.

2.7. Práctica 2: ¿Cómo autorizar el servicio DHCP Server?

IMPORTANTE: No realice esta práctica hasta haber terminado la teoría y la práctica del Capitulo 4.

Para autorizar el servicio DHCP Server, un miembro del grupo Enterprise Administrators lo agrega a una lista de DHCP Servers, los cuales pueden dar servicio a clientes DHCP en el dominio. El proceso de autorización funciona solamente con servers corriendo Windows Server 2003 y Windows 2000 en un dominio. La autorización no es posible si los DHCP Servers corren versiones anteriores como Microsoft Windows NT® u otros software DHCP Server.

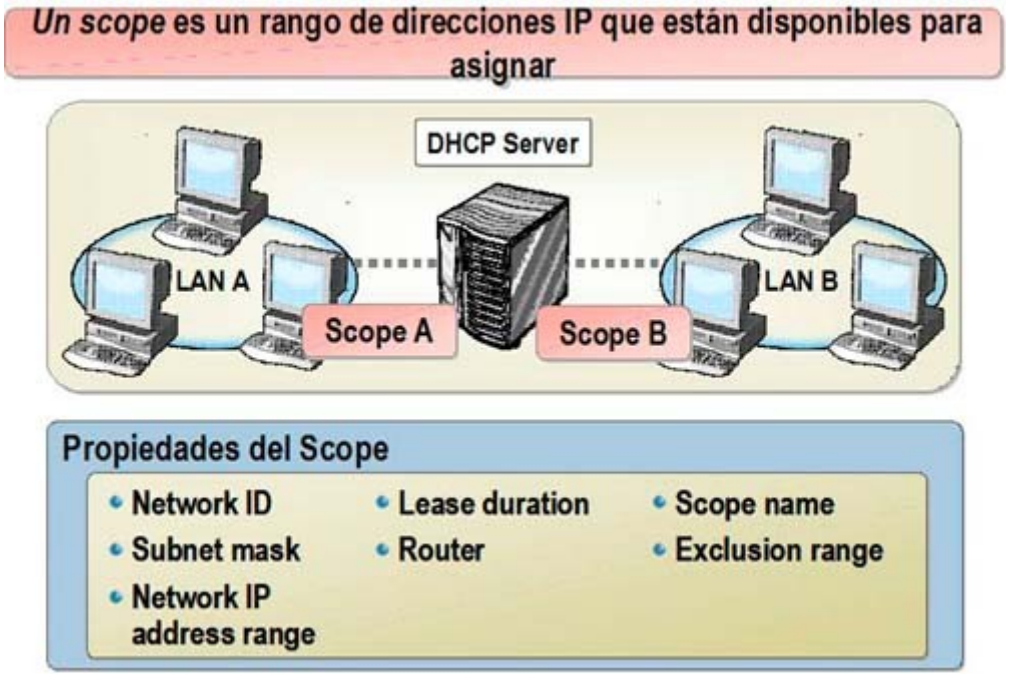
Para autorizar el servicio DHCP Server deberá:

1. Abrir la consola DHCP.
2. Seleccionar el server en la consola
3. Hacer click en ***Authorize*** del menú ***Action***,
4. Para verificar que el DHCP server esté autorizado: en la consola, presionar F5 para refrescar la vista, y verificar que el DHCP Server ahora se visualice con una flecha verde hacia arriba.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.8. ¿Qué son los DHCP Scopes?



2.8.1. Definición

Un ***scope*** es un rango de direcciones válidas IP que están disponibles para asignar a computadoras cliente en una subset en particular. Usted puede configurar un scope en el DHCP Server para determinar el pool de direcciones IP que ese server asignará a clientes.

Los scopes determinan las direcciones IP que se asignan a los clientes. Usted debe definir y activar un scope antes que los clientes puedan usar el DHCP Server para una configuración dinámica TCP/IP. Asimismo puede configurar tantos scopes en el DHCP Server como lo necesite para su ambiente de red.

2.8.2. Propiedades de Scope

Un scope tiene las siguientes características:

- ***Network ID:*** El Network ID para el rango de direcciones IP
- ***Subnet mask:*** La subnet mask para el Network ID
- ***Network IP address range:*** El rango de direcciones IP disponibles para los clientes
- ***Lease duration:*** El período de tiempo que el DHCP Server asigna a la dirección del cliente
- ***Router:*** La dirección del Default Gayeway
- ***Scope name:*** Identificador para propósitos administrativos
- ***Exclusion range:*** El rango de direcciones IP en el scope excluidas para la asignación.

Cada subnet puede tener un DHCP scope que contenga un solo y continuo rango de direcciones IP. Direcciones específicas o grupos de direcciones se pueden excluir del rango del DHCP scope. En general, solamente un scope puede ser asignado a una subnet. Si más de un scope se requiere en una subnet, los scopes deberán crearse primero y luego combinarse en un superscope.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.9. Práctica 3: ¿Cómo configurar un DHCP Scope?

Para configurar un DHCP scope:

1. Abrir la consola DHCP.
2. Hacer click en el DHCP Server de la consola.
3. Hacer click en ***New Scope*** del menú ***Action***.
4. Hacer click en ***Next*** del ***New Scope Wizard***.
5. Configurar el ***Nombre*** y ***Descripción*** en la página ***Scope Name***.
6. Configurar, en la página ***IP Address Range***, la dirección IP inicial 192.168.1.1, la dirección IP final 192.168.1.254 y la ***Subnet mask*** 255.255.255.0.
7. Configurar, en la página ***Add Exclusions***, la dirección IP inicial 192.168.1.20 y la dirección IP final 192.168.1.30, si es aplicable.
8. Configurar, en la página ***Lease Duration***, los ***Días***, ***Horas*** y ***Minutos***. (El default es 8 días).
9. Configurar ***DHCP Options*** y seleccionar ***No, I will configure these options later***.
10. Click ***Finish*** en la página ***Completing the New Scope Wizard***.

Para activar el DHCP scope:

Hacer click derecho sobre el scope de la consola, y en Activate

2.10 ¿Qué es una reserva DHCP?

Una reserva es una dirección IP permanente asignada a un cliente específico. Usted puede reservar una dirección IP permanente a un dispositivo en la red. La reserva se realiza a la dirección MAC del dispositivo.

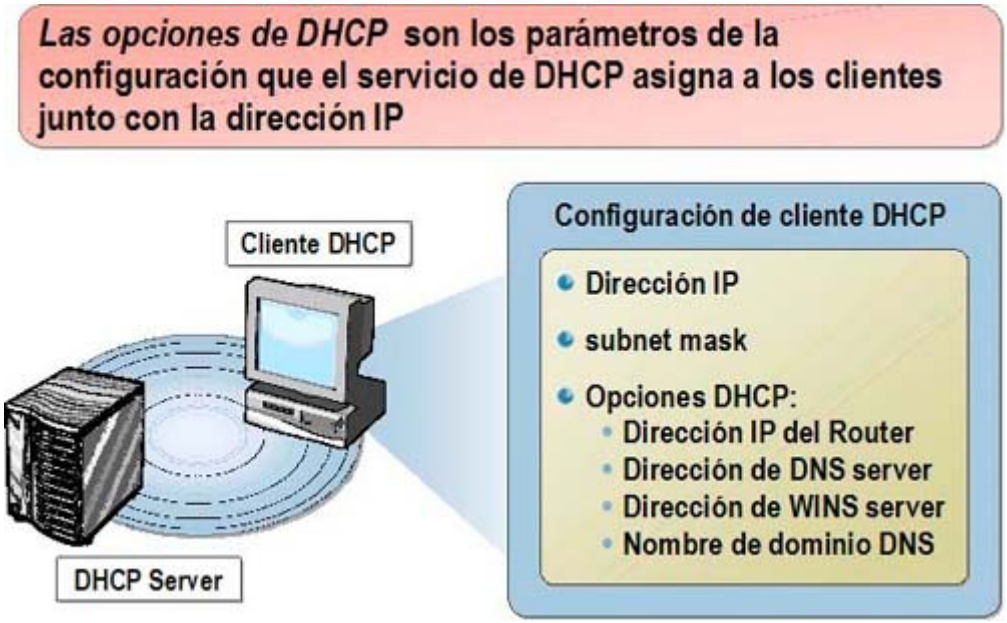
2.10.1 Práctica 4: Actividades para configurar una reserva DHCP:

1. Abrir la consola DHCP.
2. Hacer click en ***Reservations*** de la consola,
3. Hacer click en ***New Reservation*** del menú ***Action***
4. Ingresar, en el cuadro ***New Reservation***, los valores siguientes:
   a. Nombre de la reserva
   b. Dirección IP
   c. Dirección MAC (sin guiones)
   d. Descripción
5. Seleccionar, en ***Supported types***, una de las opciones siguientes:
   a. Both
   b. DHCP only
   c. BOOTP only
6. Hacer click en ***Add*** del cuadro ***New Reservations***, y después en ***Close***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio.com

2.11. ¿Qué son las opciones de DHCP?



Las opciones de DHCP son los parámetros de configuración que un servicio de DHCP asigna a los clientes cuando asigna la dirección IP.

2.11.1. Opciones comunes de DHCP

- ***Router (Default Gateway):*** Es la dirección de cualquier Default Gateway o router. El router se refiere comúnmente como Default Gateway.
- ***Domain name:*** Un Domain Name DNS define el dominio al cual pertenece una computadora cliente. La computadora cliente puede utilizar esta información para actualizar el DNS Server de modo que otras computadoras puedan localizar al cliente.
- ***DNS and WINS Servers:*** Son las direcciones de los DNS y WINS Servers para los clientes, a utilizar en la comunicación de red.

2.12. Práctica 5: ¿Cómo configurar opciones de DHCP?

Para configurar una opción de DHCP Server deberá:

1. Abrir la consola DHCP.
2. Hacer click en ***Server Options*** de la consola, bajo el nombre del server
3. Hacer click en ***Configure Options*** del menú ***Action***.
4. Seleccionar la opción que Usted desea configurar en el cuadro ***Server Options*** de la lista ***Available Options***.
5. Completar, bajo ***Data entry***, la información que se requiere para configurar esta opción.
6. Hacer click en ***OK*** del cuadro ***Server Options***.

Para configurar un scope DHCP deberá:

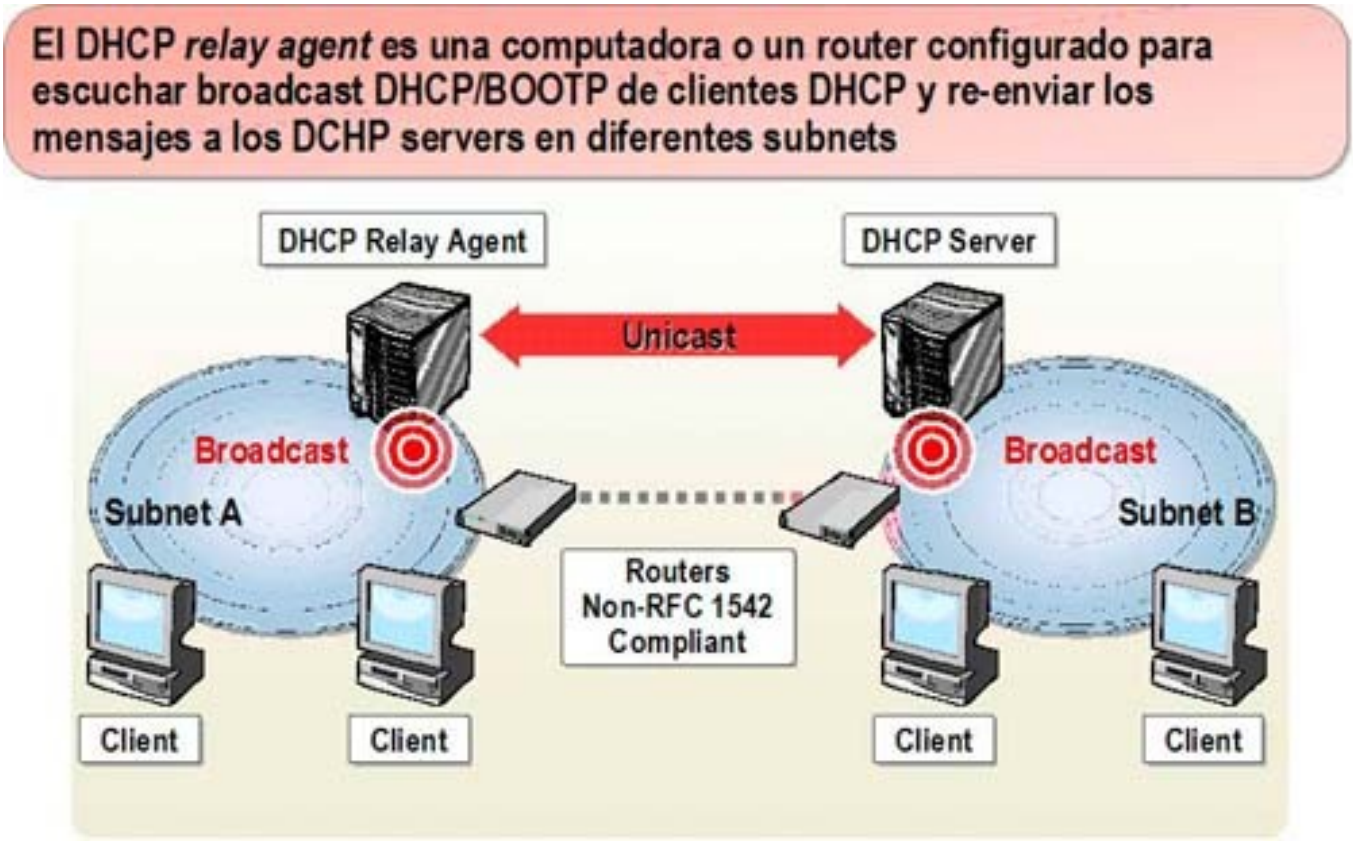
1. Abrir la consola DHCP y bajo el scope apropiado, hacer click en ***Scope Options***.
2. Hacer click en ***Configure Options*** del menú ***Action***

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3. Seleccionar, en el cuadro ***Scope Options***, la opción que usted desea configurar de la lista ***Available Options***
4. Completar, bajo ***Data entry***, la información que se requiere para configurar esta opción.
5. Hacer click en ***OK*** del cuadro ***Scope Options***.

2.13. ¿Qué es el DHCP Relay Agent?



2.13.1. Definición

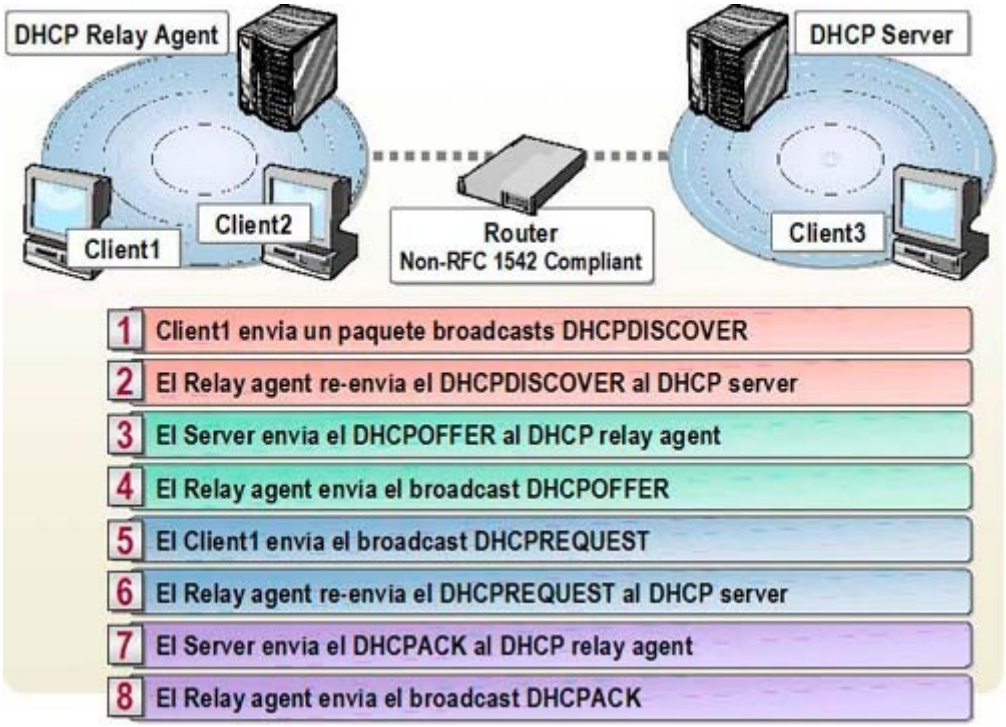
El ***DHCP Relay Agent*** es una computadora o router configurado para escuchar broadcast DHCP/BOOTP de clientes DHCP y reenviar esos mensajes a los DCHP Servers en diferentes subnets. DHCP/BOOTP Relay Agents es parte de los estándares DHCP y BOOTP, y funciona según los documentos estándar ***Request for Comments*** (RFCs) que describen el diseño del protocolo y el comportamiento relacionado.

Un ***RFC 1542-Compliant Router*** es un router que soporta el reenvío de tráfico DHCP broadcast.

Los clientes DHCP utilizan broadcasts para obtener el lease del DHCP Server. Los Routers normalmente no pasan broadcasts excepto que estén configurados específicamente para dejarlos pasar. Por lo tanto, sin configuración adicional, los DHCP Servers solo proveen direcciones IP a clientes en su subset local. Para que Usted pueda asignar direcciones a clientes en otros segmentos, deberá configurar la red para que los DHCP broadcasts puedan llegar desde el cliente al DCHP Server. Esto se puede hacer de dos maneras: configurando los routers que conectan las subnets para dejar pasar DHCP broadcasts, o configurando DCHP Relay Agents. Windows Server 2003 soporta el servicio Routing and Remote Access configurado para funcionar como DHCP Relay Agent.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso
Powered by itsitio

2.14. ¿Cómo funciona el DHCP Relay Agent?



El DHCP Relay Agent soporta el proceso Lease Generation entre el cliente DHCP y el DHCP Server, cuando se separan por un router. Esto habilita al cliente DHCP para recibir una dirección IP del DHCP Server.

Los siguientes pasos describen el funcionamiento de DHCP Reaky Agent:

1. El cliente DHCP envía un paquete broadcast DHCPDISCOVER.
2. El DHCP Relay Agent, desde la subnet del cliente, reenvía el mensaje DHCPDISCOVER al DHCP Server usando unicast.
3. El DHCP Server usa unicast para enviar el mensaje DHCPOFFER al DHCP Relay Agent.
4. El DHCP Relay Agent envía un paquete broadcast DHCPOFFER al cliente DHCP en su subnet.
5. El cliente DHCP envía un paquete broadcast DHCPREQUEST.
6. El DHCP Relay Agent, desde la subnet del cliente, reenvía el mensaje DHCPREQUEST al DHCP Server, usando unicast.
7. El DHCP Server usa unicast para enviar el mensaje DHCPACK al DHCP Relay Agent.
8. El DHCP Relay Agent envía un paquete broadcast DHCPACK al cliente DHCP en su subnet.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.14.1 Práctica 6: ¿Cómo configurar el DHCP Relay Agent?

Para agregar un DHCP Relay Agent deberá:

1. Abrir la consola Routing and Remote Access.
2. Hacer click derecho en el server y después en ***Configure and Enable Routing and Remote Access***.
3. Hacer click en Next de la pantalla del wizard ***Welcome to the Routing and Remote Access Server Setup Wizard***.
4. Seleccionar ***Custom configuration*** en la página ***Configuration***, y hacer click en ***Next***.
5. Seleccionar ***LAN routing*** en la página ***Custom Configuration*** y hacer click en ***Next***.
6. Hacer click en ***Finish*** de la página ***Completing the Routing and Remote Access Server Setup Wizard***.
7. Hacer click en ***Yes*** del cuadro de advertencia de ***Routing and Remote Access***, para iniciar el servicio.
8. Hacer click en ***Finish*** de la página ***This Server is Now a Remote Access/VPN Server***
9. Expandir el server y el ***IP Routing*** en la consola, y seleccionar ***General***.
10. Hacer click derecho en ***General*** y después en ***New Routing Protocol***.
11. Hacer click en ***DHCP Relay Agent*** del cuadro ***New Routing Protocol*** y después en ***OK***.

Para configurar la dirección IP del DHCP Server en el DHCP Relay Agent deberá:

12. Abrir la consola Routing and Remote Access.
13. Seleccionar ***DHCP Relay Agent*** en la consola.
14. Hacer click derecho en ***DHCP Relay Agent*** y después en ***Properties***.
15. Ingresar la dirección IP del DHCP Server al que quiere enviar los pedidos DHCP, en ***General*** del campo ***Server address***.
16. Hacer click en ***Add***, y después en ***OK***.

Para habilitar el DHCP Relay Agent en una interfase del router deberá:

17. Abrir la consola ***Routing and Remote Access***.
18. Seleccionar ***DHCP Relay Agent*** en la consola
19. Hacer click derecho en ***DHCP Relay Agent*** y después en ***New Interface***.
20. Seleccionar la interfase donde quiere habilitar el DHCP Relay Agent, y después hacer click en ***OK***.
21. Verificar si está seleccionado el cuadro ***Relay DHCP packets*** en ***General*** del cuadro ***DHCP Relay Properties***, en ***General***.

Para obtener más información acerca de DHCP:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323416

http://support.microsoft.com/default.aspx?scid=kb;en-us;325473

http://support.microsoft.com/default.aspx?scid=kb;en-us;306104

http://support.microsoft.com/default.aspx?scid=kb;en-us;323360

http://support.microsoft.com/default.aspx?scid=kb;en-us;323355

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3. Descripción de Domain Name System

DNS es un servicio de resolución de nombres que resuelve direcciones legibles (como www.microsoft.com) en direcciones IP (como 192.168.0.1).

Domain Name System (DNS) es una base de datos jerárquica distribuida, que contiene mapeos de nombres de host DNS a direcciones IP. DNS habilita la localización de computadoras y servicios usando nombres alfanuméricos, más fáciles de recordar. DNS también habilita la localización de servicios de red, como E-mail Servers y Domain Controllers en Active Directory®.

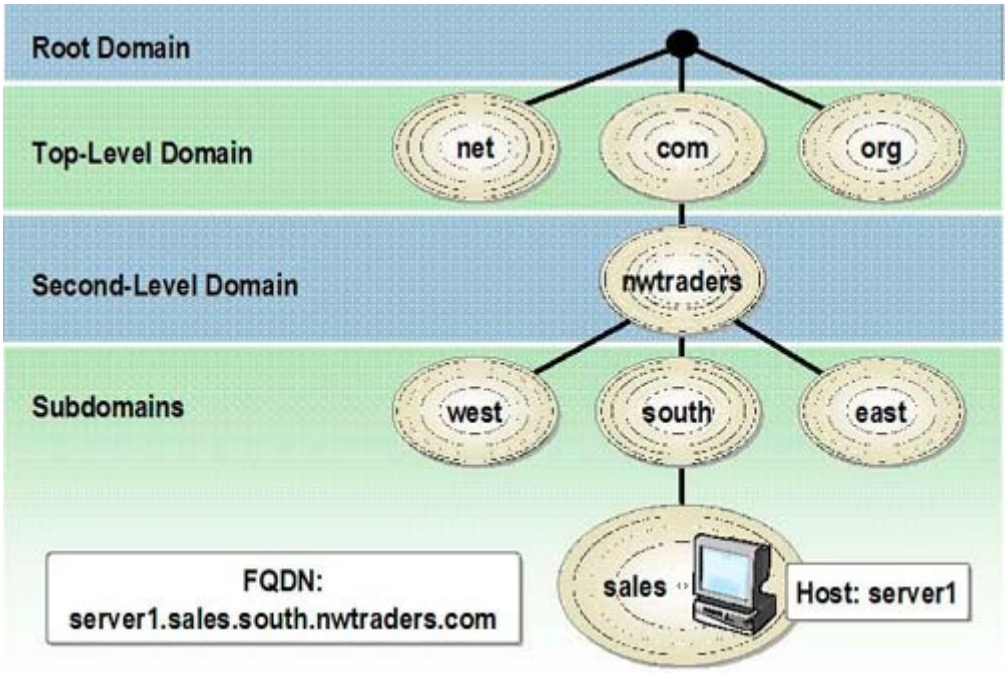
Con DNS, los nombres de host residen en una base de datos distribuida en múltiples servers, disminuyendo la carga en un servidor y la capacidad para administrar este sistema de nombres. Asimismo, dado que se distribuye la base de datos de DNS, su tamaño es ilimitado y el funcionamiento no se degrada cuanto más servidores se agregan.

InterNIC es responsable de delegar la responsabilidad administrativa de porciones del Namespace de dominio, y también de registrar nombres de dominio. Estos últimos son administrados a través del uso de la base de datos distribuida y almacenada en Name Servers, localizados en toda la red. Cada Name Server contiene archivos de base de datos que poseen información para una región, dominio etc., creando así la jerarquía.

Para obtener más información acerca de InterNic:

http://www.internic.net

3.1 ¿Qué es el Domain Namespace?



El ***Domain Namespace*** es un árbol de nombres jerárquico que utiliza DNS para identificar y localizar un host en un dominio dado, concerniente a la raíz del árbol. Los nombres en la base de datos DNS establecen una estructura lógica llamada Domain Namespace, que identifica la posición de un dominio en el árbol y su

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

dominio superior. La convención principal es simplemente ésta: para cada nivel de dominio, un período (.) se utiliza para separar a cada descendiente del subdominio y de su dominio de nivel superior.

El ***Fully Qualified Domain Name (FQDN)*** es el nombre de dominio DNS que indica con certeza la localización del host al que se refiere, y su ubicación en el Domain Namespace.

3.1.1 Práctica 7: ¿Cómo instalar el servicio DNS Server?

Para agregar un DNS Server, Usted debe instalar DNS service en una computadora corriendo Microsoft® Windows® Server 2003.

Antes de agregar el servicio DNS Server deberá:

- Verificar que la configuración IP en el servidor esté correcta.
- Verificar que la configuración IP del servidor contenga una dirección IP estática, una subset mask y un Default Gateway en ambientes ruteados.
- Verificar que la cuenta de usuario tenga los permisos correctos.

Para agregar el servicio DNS Server deberá:

1. Iniciar sesión usando una cuenta no-administrativa.
2. Hacer click en ***Start*** y después en ***Control Panel***.
3. Abrir las ***Administrative Tools*** en el ***Control Panel*** y hacer click derecho en ***Manage Your Server***, seleccionando ***Run as***.
4. Seleccionar ***The following user*** en el cuadro ***Run As***, ingresar una cuenta de usuario y password que tenga los permisos apropiados para realizar la tarea, y hacer click en ***OK***.
5. Hacer click en ***Add or remove a role*** de la ventana Manage Your Server.
6. Hacer click en ***Next*** de la página ***Preliminary Steps***.
7. Seleccionar ***DNS server*** en el wizard ***Configure Your Server***, y hacer click en ***Next***.
8. Hacer click en ***Next*** de la página ***Summary of Selections***,
9. Ingresar el CD Microsoft Windows Server 2003, si se lo pide.
10. Hacer click en ***Cancel*** de la página ***Welcome to the Configure a DNS Server Wizard***,
11. Hacer click en ***Finish*** de la página ***Configure Your Server wizard***.

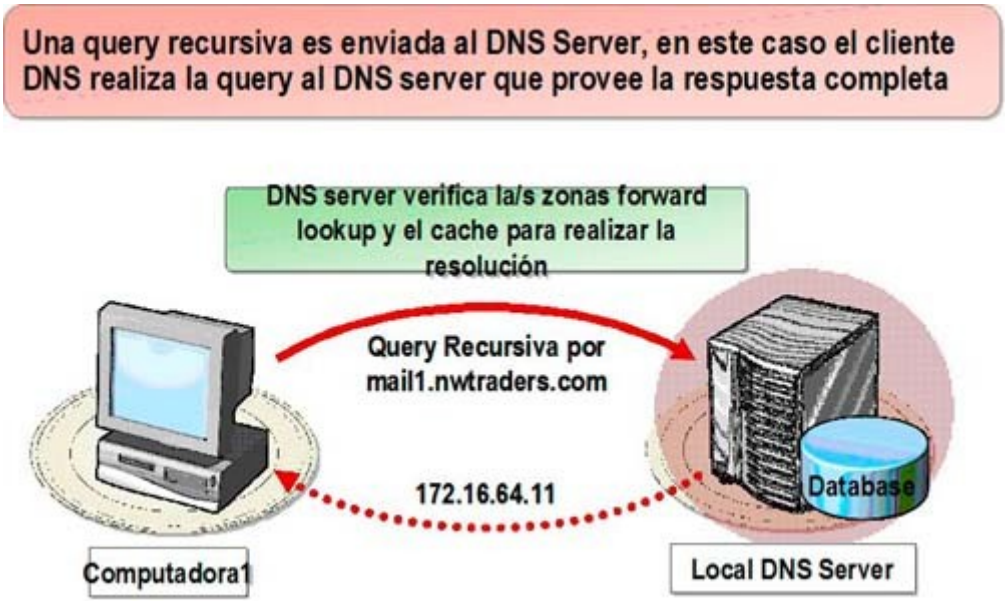
3.2 ¿Qué es una Query DNS?

Una ***Query*** es una solicitud de resolución de nombre enviado a un DNS Server. Hay dos tipos de Query: Recursiva e Iterativa.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

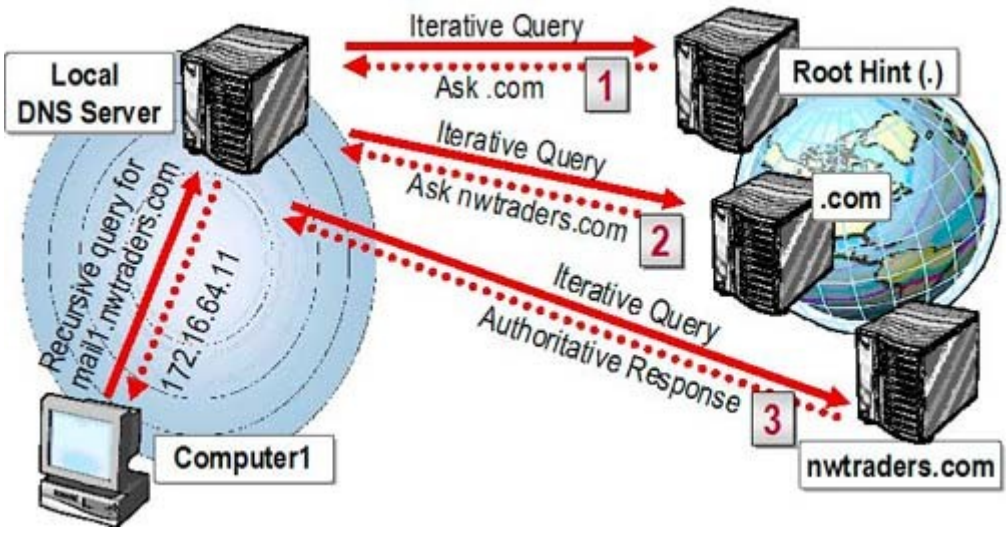
Powered by itsitio

3.2.1 ¿Cómo funciona una Query Recursiva?



Una ***Query Rrecursiva*** es una solicitud de resolución al DNS Server, en el caso que el cliente realice la Query directamente al DNS Server. La única respuesta aceptable a una Query Recursiva es la respuesta completa o la respuesta en donde el nombre no puede ser resuelto. Una Query Recursiva nunca se redirecciona a otro DNS Server. Si el DNS consultado no obtiene la respuesta de su propia base o del cache, la respuesta es un error, indicando que no puede resolver el nombre.

3.2.2 ¿Cómo funciona una Query Iterativa?



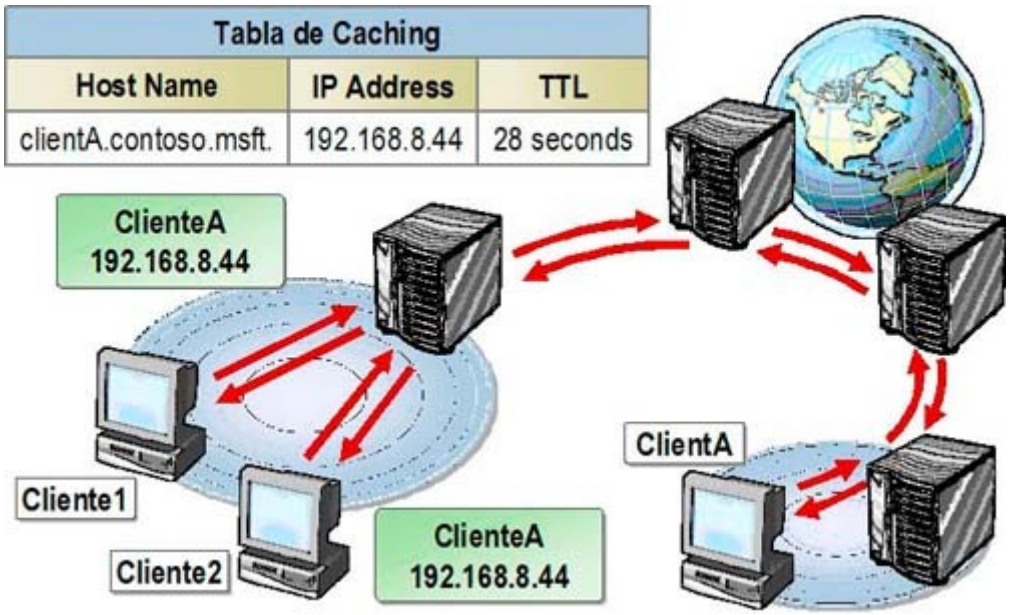
A diferencia de las Querys Recursivas, cuando un cliente realiza un pedido de resolución y el DNS Server no obtiene la respuesta de su propia base o del cache, la Query Iterativa consulta a otros DNS Servers en nombre del cliente para devolver la respuesta. Ejemplo: si usted necesita acceder a un

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

sitio Web en Internet, normalmente consultaría al DNS de su ISP, y éste último se encargaría de contactar a otros DNS Servers hasta lograr la respuesta. Pero analice lo siguiente: es imposible en Internet que el DNS de su ISP contenga todas las resoluciones posibles en toda la red Internet, y por eso las bases de DNS se distribuyen y se resuelven nombres de forma Iteractiva.

3.2.3 ¿Cómo funciona el caching de DNS Server?



Caching es el proceso temporal de almacenar la información reciente, y resulta en un subsistema especial de la memoria para un acceso más rápido.

Cuando un server está procesando una Query Recursiva, puede ser que se requiera enviar varias Querys para encontrar la respuesta definitiva. En el peor de los casos para resolver un nombre, el server local comienza en el Root DNS y trabaja hacia abajo hasta que encuentra los datos solicitados.

El server guarda la información de la resolución en su cache por un tiempo determinado. Este periodo de tiempo se denomina Time to Live (TTL) y es especificado en segundos. El administrador del server que contiene la primary zone donde están los datos, decide el valor del TTL. Cuanto más pequeño sea el valor del TTL, le ayudará a mantener datos más consistentes en caso de cambios. Sin embargo, esto también generará más carga de trabajo sobre el Name Server.

Después que el DNS Server guarda en cache los datos, el TTL comienza a decrecer hacia abajo hasta llegar a 0 (zero) y en ese punto el registro es eliminado del cache de DNS Server. Mientras el valor de TTL está activo, el DNS Server resuelve los pedidos utilizando el registro de cache.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

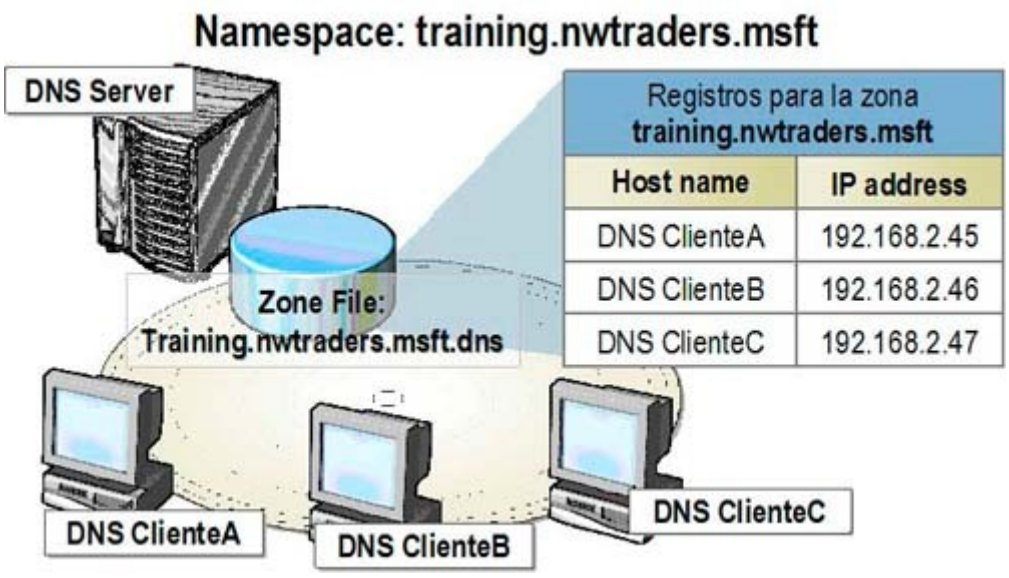
3.3. Práctica 8: ¿Cómo configurar propiedades del servicio DNS Server?

Para configurar propiedades del servicio DNS Server, Usted necesita actualizar los Root Hints en el DNS Server. Los Root Hints determinan si su server consulta a los root de Internet o si el root es un server interno.

Para actualizar los Root Hints en el DNS Server deberá:

1. Abrir la consola de DNS.
2. Seleccionar el server apropiado en la consola DNS.
3. Hacer click en ***Properties*** del menú ***Action***.
4. En ***Root Hints***, Usted puede hacer click en:
   - ***Add***, para agregar un Name Server. Agregue la IP de su server.
   - ***Edit***, para editar un Name Server.
   - ***Remove***, para quitar un Name Server.
   - ***Copy from Server***, para copiar la lista de Name Servers desde otro DNS Server.
5. Hacer click en ***OK*** para cerrar el cuadro ***Properties***.
6. Cerrar la consola DNS

3.4 ¿Cómo se almacenan y se mantienen los datos DNS?



Una ***zona*** es una parte contigua del espacio de nombres de dominio en el que un servidor DNS tiene autoridad para resolver consultas DNS. El espacio de nombres DNS se puede dividir en diferentes zonas, que almacenan información de nombres acerca de uno o varios dominios DNS, o partes de ellos. Para cada nombre de dominio DNS incluido en una zona, ésta se convierte en el origen autorizado de la información acerca de ese dominio.

Antes de crear zonas, debe comprender los siguientes conceptos:

- ***Tipos de zonas.*** Los servidores DNS pueden alojar varios tipos de zona. Para limitar el número de servidores DNS en la red, puede configurar uno solo que admita o aloje varias zonas. También puede configurar varios servidores para alojar una o varias zonas con el fin de proporcionar tolerancia a errores y distribuir la carga de trabajo administrativa y de resolución de nombres.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

- ***Archivo de zona.*** Los registros de recursos que se almacenan en un archivo de zona definen a ésta. El archivo de zona almacena información que se utiliza para convertir nombres de host en direcciones IP y viceversa.

Importante: Para crear zonas y administrar un servidor DNS que no se ejecuta en un controlador de dominio, debe ser miembro del grupo de administradores en ese equipo. Para configurar un servidor DNS que se ejecuta en un controlador de dominio, debe ser miembro de los grupos administradores de DNS, administradores de dominio o administradores Enterprise.

3.4.1. Identificación de tipos de zonas

Zonas	Descripción
Primary	Copia Read/write de una base de datos DNS
Secondary	Copia Read-only de una base de datos DNS
Stub	Copia de una zona conteniendo recursos limitados

En la tabla siguiente se describen los cuatro tipos de zonas que se pueden configurar, así como los archivos de zona asociados con ellas.

Estándar Principal: Contiene una versión de lectura y escritura del archivo de zona que se almacena en un archivo de texto estándar. Los cambios realizados en la zona se registran en dicho archivo.

Estándar Secundario: Contiene una versión de sólo lectura del archivo de zona que se almacena en otro archivo de texto estándar. Los cambios efectuados en la zona se registran en el archivo de zona principal y se replican en el archivo de zona secundaria. Cree una zona secundaria estándar para crear una copia de una zona existente y de su archivo de zona. De esta forma se puede distribuir la carga de trabajo de la resolución de nombres entre varios servidores DNS.

Integrada de Active Directory: En lugar de almacenar la información de zona en un archivo de texto, se almacena en Active Directory. Las actualizaciones de la zona se producen automáticamente durante la replicación de Active Directory. Cree una zona integrada de Active Directory para simplificar el planeamiento y la configuración de un espacio de nombres DNS. No es necesario configurar servidores DNS para especificar cómo y cuándo se producen las actualizaciones, ya que Active Directory mantiene la información de zona.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Zona Stub: La zona Stub son las copias de una zona que contienen solamente los registros que son necesarios identificar en el server autoritativo DNS para esa zona. Una zona stub contiene un subconjunto de datos de la zona que consisten en registros SOA, NS, y A. Las zona Stub puede ser utilizada donde un servidor interno DNS representa al Root en lugar de los Root Servers de Internet.

3.4.1.1 Zonas Estándar Principales

El servidor principal de una zona actúa como punto de actualización de la zona. Las zonas recién creadas son siempre de este tipo. Con Windows Server 2003, las zonas principales se pueden utilizar de una de dos formas: como zonas estándar principales o como zonas principales integradas con Active Directory. En las zonas estándar principales, sólo un servidor puede alojar y cargar la copia maestra de la zona. Si crea una zona y la mantiene como zona estándar principal, no se permite ningún servidor principal adicional para la zona. Sólo un servidor puede aceptar actualizaciones dinámicas y procesar los cambios de zona.

El modelo principal estándar supone un punto de concentración de errores. Por ejemplo, si por cualquier motivo el servidor principal de una zona no está disponible para la red, no se puede realizar ninguna actualización dinámica de la zona. Tenga en cuenta que las consultas de nombres en la zona no se ven afectadas y pueden continuar sin interrupción, siempre y cuando los servidores secundarios de la zona estén disponibles para responderlas.

La adición de una nueva zona principal a un servidor existente puede llevarse a cabo siempre que se necesiten dominios o subdominios adicionales en el espacio de nombres de dominio DNS. Por ejemplo, podría tener una zona para un dominio de segundo nivel como microsoft.com y desear agregar una zona principal para el nuevo subdominio como nwtraders.msft. En este ejemplo puede crear la zona nueva para el subdominio con el Asistente para configuración de zona nueva del complemento DNS. Cuando haya finalizado, debe crear una delegación en la zona principal del nuevo dominio (como la zona microsoft.com) para completar la adición del nuevo subdominio y su zona principal.

En las zonas principales estándar, algunas veces puede ser necesario cambiar el servidor principal designado para una zona. Por ejemplo, supongamos que el servidor principal actual de una zona principal estándar es Servidor A y el nuevo servidor principal de la zona es Servidor B. Para influir en el cambio de estado del Servidor A al Servidor B, realice los siguientes cambios de zona:

1. Agregue un nuevo registro de recursos (RR) de host (A) para el Servidor B.
2. Actualice el registro de recursos de servidor de nombres (NS) de la zona para quitar el Servidor A e incluir el Servidor B como servidor autorizado y configurado, que apunta al nuevo registro de recursos RR A agregado en el paso 1.
3. Revise el nombre del campo de propietario del registro de recursos de inicio de autoridad (SOA) para la zona del Servidor A al Servidor B.
4. Quite el registro de recursos A antiguo del Servidor A.
5. Compruebe la zona principal para asegurarse que los registros de delegación (registros de recursos NS o A) utilizados se actualizan para hacer referencia al Servidor B.

3.4.1.2 Zonas Estándar Secundarias

Las especificaciones de diseño de DNS recomiendan el uso de al menos dos servidores DNS para alojar cada zona. Para las zonas de tipo estándar principal, se necesita un servidor secundario para agregar y configurar la zona que aparece ante otros servidores DNS de la red. Los servidores secundarios pueden proporcionar un medio para aliviar el tráfico de consultas DNS en áreas de la red en las que una zona se consulta y utiliza mucho. Además, si un servidor principal deja de ser operativo, un servidor secundario puede realizar parte de la resolución de nombres en la zona hasta que el servidor principal esté disponible.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

Si agrega un servidor secundario, intente ubicarlo lo más cerca posible de los clientes que requieran muchos nombres en la zona. Además, es recomendable colocar servidores secundarios a través de un router, ya sea en otras subredes (si se utiliza una LAN ruteada) o en vínculos WAN. De esta manera, se usa eficazmente un servidor secundario como copia de seguridad local en aquellos casos en los que un vínculo de red intermedio se convierte en un punto de concentración de errores entre servidores y clientes DNS que utilizan la zona.

Como el servidor principal siempre mantiene la copia maestra de las actualizaciones y cambios efectuados en la zona, el servidor secundario depende de mecanismos de transferencia de zonas DNS para obtener su información y mantenerla actualizada. Algunas cuestiones como los métodos de transferencia de zona, ya sea mediante transferencias de zona completas o incrementales, se simplifican cuando se utilizan servidores secundarios. Al considerar el impacto de las transferencias de zona causadas por los servidores secundarios, tenga en cuenta su ventaja como origen de copia de seguridad de información y compárela con el costo agregado que suponen en la infraestructura de red.

Una regla sencilla es que por cada servidor secundario que se agrega, aumenta el uso de la red (debido al tráfico adicional generado en la replicación de zona) y el tiempo necesario para sincronizar la zona en todos los servidores secundarios.

3.4.1.3 Zonas Integradas de Active Directory

En Windows Server 2003 puede agregar más servidores principales para una zona, mediante las características integradas de almacenamiento y replicación de directorios del servicio DNS. Para ello, es necesario cambiar una zona e integrarla en Active Directory.

Para integrar una zona existente en Active Directory, cambie el tipo de una zona en el servidor principal de origen donde se creó por primera vez. Una vez que el tipo de zona haya cambiado de estándar principal a Integrada de Active Directory, podrá agregar la zona a otros servidores DNS. A tal efecto, deberá configurarlos de modo que usen la opción para iniciar desde servicios de directorio cuando inicialicen el servicio DNS.

Cuando se selecciona esta opción, otros servidores DNS que funcionan como controladores de dominio para el dominio de Active Directory pueden consultar el directorio y cargar automáticamente todas las zonas integradas de él, que se almacenan en la base de datos de directorios. No se requiere ningún otro paso. Cualquier servidor DNS que funcione como parte de Active Directory es también, de manera predeterminada, servidor principal para las zonas integradas de directorio.

En las zonas principales integradas de directorio, los servidores secundarios se admiten pero no son necesarios para ofrecer tolerancia a errores. Por ejemplo, dos servidores DNS que funcionan como controladores de dominio de Windows Server 2003 pueden ser servidores principales redundantes para una zona y ofrecer las mismas ventajas que supone agregar un servidor secundario, además de otras adicionales.

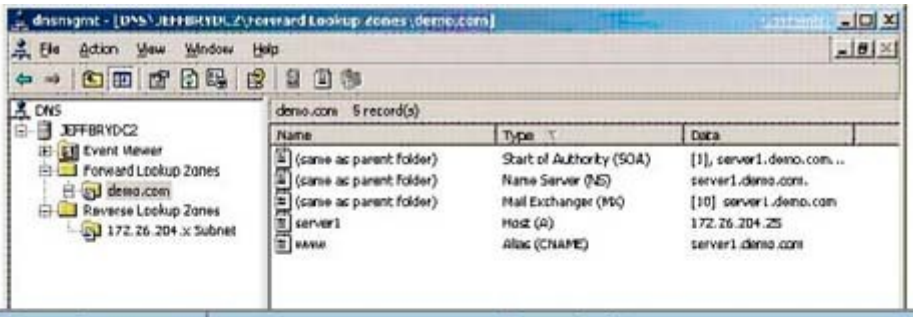
Como el archivo de zona se mantiene en el contexto de nombres de dominio de Active Directory, los controladores de dominio deben estar en el mismo dominio para actuar como servidores principales redundantes en una zona. Cuando sea necesario compartir esta información de zona entre dominios, deberá crearse un servidor de zona secundaria estándar.

Nota: Este tipo de zona se verá más claramente en el capítulo 4 "Active Directory".

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.5 ¿Qué son Resource Records y Record Types?



Record type	Descripción
A	Resuelve nombres de host name a IP
PTR	Resuelve IP a nombres host
SOA	El primer registro en cualquier archivo de zona
SRV	Resuelve nombres de servers que proveen servicios
NS	Identifica el DNS server para cada zona
MX	El server de mail
CNAME	Resoluciones desde nombres de host a nombres de host

Los archivos de zona contienen la información a la que un servidor DNS hace referencia para realizar dos tareas distintas: convertir nombres de host en direcciones IP y convertir direcciones IP en nombres de host. Esta información se almacena como registros de recursos que llenan el archivo de zona. Un archivo de zona contiene los datos de resolución de nombres para una zona, incluidos los registros de recursos con información para responder a consultas DNS. Los registros de recursos son entradas de base de datos que incluyen varios atributos de un equipo, como el nombre de host o el nombre de dominio completo, la dirección IP o el alias.

Los servidores DNS pueden contener los siguientes tipos de registros de recursos:

A (host): Contiene la información de asignaciones de nombre a dirección IP, que se utiliza para asignar un nombre de dominio DNS a una dirección IP de host en la red. Los registros de recursos A también se conocen como registros de host.

NS (name server): Designa los nombres de dominio DNS de los servidores que tienen autoridad en una zona determinada o que contienen el archivo de zona de ese dominio.

CNAME (canonical name): Permite proporcionar nombres adicionales a un servidor que ya tiene un nombre en un registro de recursos A. Por ejemplo, si el servidor llamado webserver1.nwtraders.msft aloja el sitio web de nwtraders.msft, debe tener el nombre común ww.nwtraders.msft. Los registros de recursos CNAME también se conocen como registros de alias.

MX (mail exchanger): Especifica el servidor en el que las aplicaciones de correo electrónico pueden entregar correo. Por ejemplo, si tiene un servidor de correo que se ejecuta en un equipo llamado mail1.nwtraders.msft y desea que todo el correo de nombreDeUsuario@nwtraders.msft se entregue en este servidor, es necesario que el registro de recursos MX exista en la zona de nwtraders.msft y apunte al servidor de correo de ese dominio.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

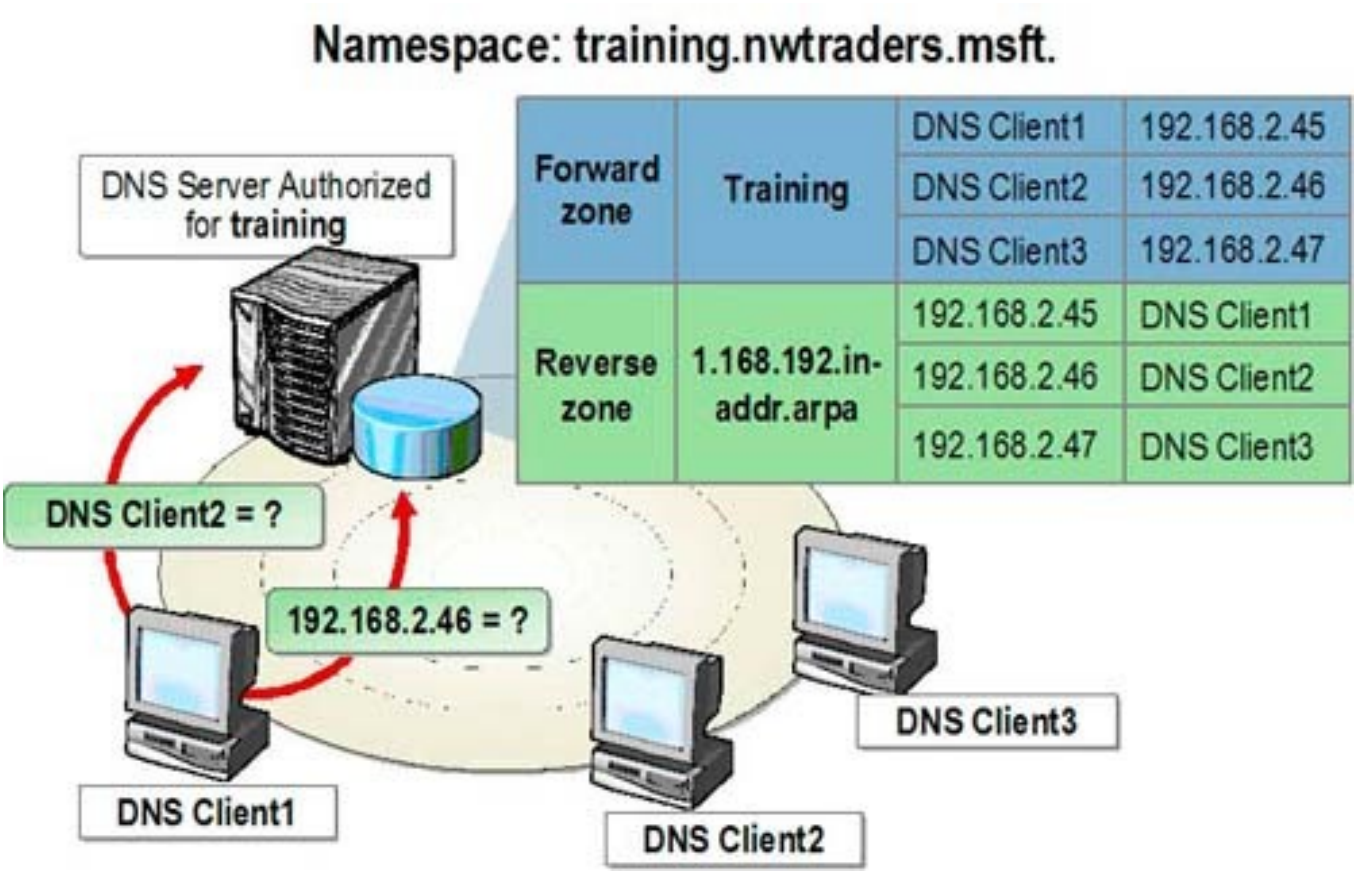
Powered by

SOA (Start Authority): Indica el punto de partida o el punto original de autoridad para la información almacenada en una zona. El registro de recursos SOA es el primero que se crea cuando se agrega una zona nueva. Contiene también varios parámetros que utilizan otros equipos que emplean DNS para determinar cuánto tiempo utilizarán la información de la zona y con cuánta frecuencia hay que realizar actualizaciones.

PTR (pointer): Se utiliza en una zona de búsqueda inversa creada en el dominio in-addr.arpa para designar una asignación inversa de una dirección IP de host a un nombre de dominio DNS de host.

SRV (service): Lo registran los servicios para que los clientes puedan encontrar un servicio mediante DNS. Los registros SRV se utilizan para identificar servicios en Active Directory y también se conocen como registros de ubicación de servicio.

3.6 Creación de zonas de búsqueda estándar



En la mayoría de las búsquedas de DNS los clientes suelen realizar una búsqueda directa, que es una solicitud para asignar un nombre de equipo a una dirección IP. DNS proporciona también un proceso de búsqueda inversa, que permite a los clientes solicitar un nombre de equipo en función de la dirección IP del equipo.

3.6.1. Creación de una zona de búsqueda directa

Para crear una zona de búsqueda directa, haga click en ***Búsqueda directa*** en la página ***Zona de búsqueda directa o inversa*** del Asistente para zona nueva. El asistente lo guía por el proceso de asignar un nombre a la zona y al archivo de zona, y asimismo crea automáticamente la zona, el archivo de zona y los registros de recursos necesarios para el servidor DNS en el que se crea la zona.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.6.2. Creación de una zona de búsqueda inversa

Para crear una zona de búsqueda inversa, haga click en ***Búsqueda inversa*** en la página ***Zona de búsqueda directa o inversa*** del Asistente para zona nueva. El asistente le indica cómo especificar la identificación de la red o el nombre de zona y cómo comprobar el nombre del archivo de zona según la información de identificación de la red. Asimismo crea automáticamente la zona, el archivo de zona y los registros de recursos necesarios para el servidor DNS en el que se crea la zona.

El dominio in-addr.arpa es un dominio DNS especial de nivel superior que está reservado para la asignación inversa de direcciones IP en nombres de host DNS. Para crear el espacio de nombres inverso, se forman subdominios en el dominio in-addr.arpa con el orden inverso de los números en notación decimal con puntos de las direcciones IP.

Para cumplir los estándares RFC, el nombre de la zona de búsqueda inversa requiere el sufijo de dominio in-addr.arpa. Al crear una zona de búsqueda inversa, este sufijo se agrega automáticamente al final de la identificación de la red. Por ejemplo, si la red utiliza el identificador de red de clase B 172.16.0.0, el nombre de la zona de búsqueda inversa se convierte en 16.172.in-addr.arpa.

3.7. Configuración de zonas estándar

Para cada zona, el servidor que mantiene los archivos de zona principal estándar se llama ***servidor principal***, y los servidores que alojan los archivos de zona secundaria estándar se llaman ***servidores secundarios***. Un servidor DNS puede alojar el archivo de zona principal estándar (como servidor principal) de una zona y el archivo de zona secundaria estándar (como servidor secundario) de otra zona.

Puede configurar uno o varios servidores DNS para alojar:

- Una o varias zonas principales estándar.
- Una o varias zonas secundarias estándar.
- Una combinación de zonas principales estándar y zonas secundarias estándar.

Nota: Para crear una zona secundaria estándar, debe crear primero una zona principal estándar.

3.7.1 Especificación de un Master Server DNS para una zona secundaria

Al agregar una zona secundaria estándar, debe designar uno o varios servidores DNS en donde obtener la información de zona. El servidor o servidores designados se conocen como Master Servers

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

DNS. Un ***Master Server DNS*** transfiere información de zona al servidor DNS secundario. Usted puede designar un servidor principal u otro servidor secundario como Master Server DNS para una zona secundaria estándar.

Para especificar un Master Server DNS en la página Masters Servers del Asistente para zona nueva, escriba la dirección IP del Master Server en el cuadro Dirección IP y haga click en Agregar.

3.8 Práctica 9: Configurando zonas DNS

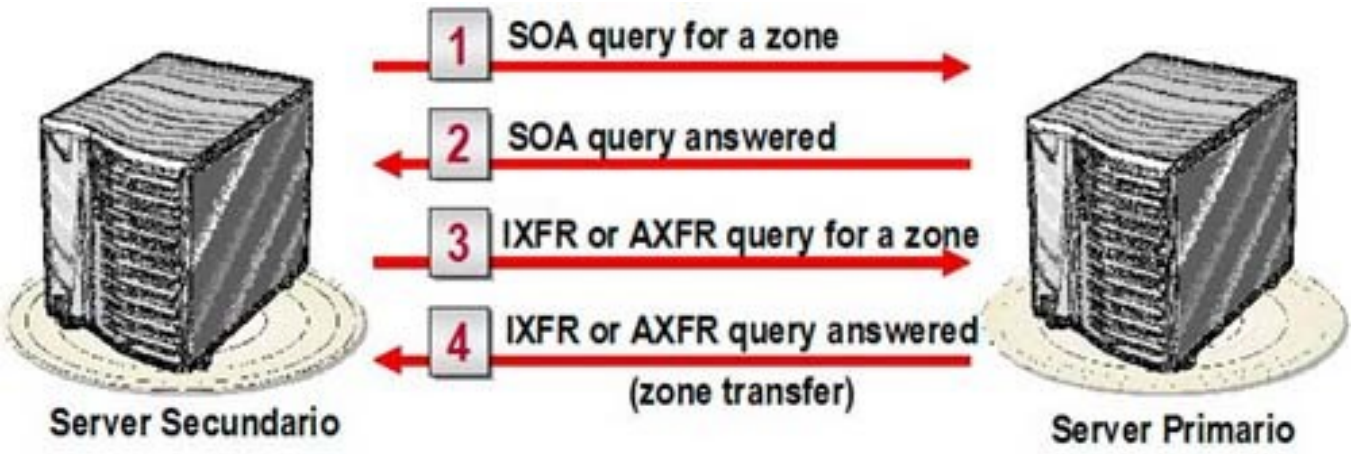
Configurar una zona de búsqueda del tipo primario

Nombre de zona: ***nwtraders.msft***

Después de terminar esta tarea, obtendrá una zona primaria configurada.

1. Abrir la consola DNS.
2. Hacer click derecho en el DNS Server de la consola DNS, y después en ***New Zone***.
3. Hacer click en ***Next*** de la página ***Welcome to the New Zone Wizard***
4. Seleccionar ***Primary zone*** en la página ***Zone Type*** y después hacer click en ***Next***.
5. Seleccionar ***Forward lookup zone*** en la página ***Forward or Reverse Lookup Zone***, y después hacer click en ***Next***.
6. Ingresar el nombre DNS para la zona en la página ***Zone Name***, y hacer click en ***Next***.
7. Hacer click en ***Next*** de la página ***Zone File*** para aceptar los defaults.
8. Hacer click en ***Finish*** de la página ***Completing the New Zone Wizard***.
9. Cerrar la consola DNS.

3.9. Proceso de transferencia de zona



Para proporcionar disponibilidad y tolerancia a errores en la resolución de nombres, los datos de la zona deben estar disponibles desde más de un servidor DNS de una red. Por ejemplo, si se utiliza un solo servidor DNS y éste no responde, las consultas de nombres fallarán. Cuando se configura más de un servidor para alojar una zona, se requieren transferencias de zona para replicar y sincronizar los datos de la zona entre todos los servidores que están configurados para alojarla.

3.9.1. Transferencia de zona

La ***transferencia de zona*** es el proceso en el que un archivo de zona se replica en otro servidor DNS. Las transferencias de zona se producen cuando las asignaciones de nombres y direcciones IP

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

cambian en el dominio. Cuando esto ocurre, los archivos de zona modificados se copian desde un Master Server a sus servidores secundarios.

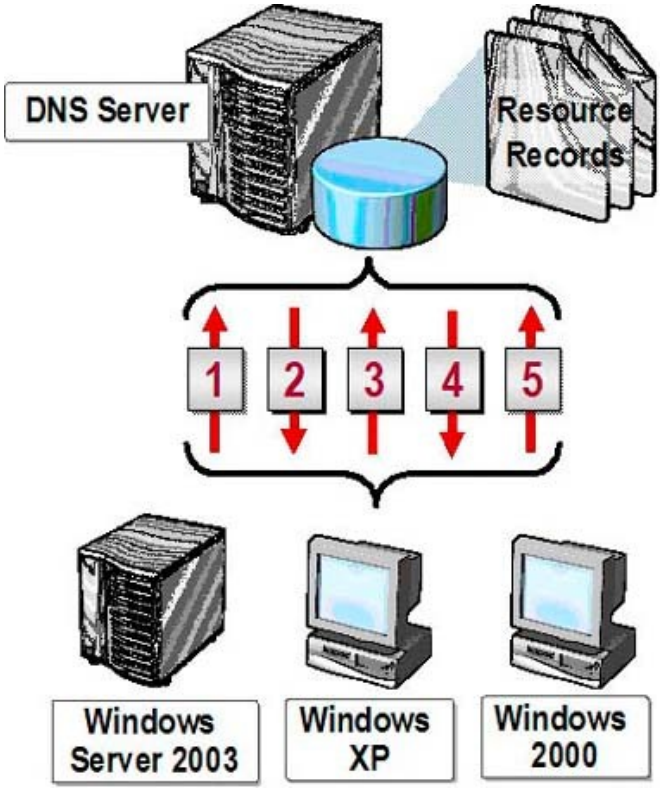
3.9.2. Transferencia de zona incremental

En Windows Server 2003, la información de una zona se actualiza mediante ***transferencias de zona incrementales (IXFR)***, que sólo replican los cambios realizados en el archivo de zona, en lugar de replicar todo el archivo. Los servidores DNS que no admiten IXFR solicitan el contenido entero de un archivo de zona cuando inician una transferencia de zona. Esto se conoce como AXFR o ***transferencia de zona completa***.

El proceso de transferencia de zona se inicia cuando se produce una de las siguientes situaciones:

- Un servidor maestro envía al servidor o servidores secundarios una notificación anunciando que se ha producido un cambio en la zona. Cuando el servidor secundario recibe la notificación, consulta los cambios en el Master Server.
- Cada servidor secundario consulta periódicamente un servidor maestro para comprobar si hubo cambios en el archivo de zona, incluso si no se le ha notificado ningún cambio. Esto ocurre cuando se inicia el servicio Servidor DNS en el servidor secundario o cuando transcurre el intervalo de actualización en el servidor secundario.

3.10. Introducción a las actualizaciones dinámicas



Usted puede configurar servidores DHCP para asignar automáticamente direcciones IP a equipos cliente. Cuando un cliente recibe una nueva dirección IP de un servidor DHCP, se debe actualizar la información de asignaciones de nombres a direcciones IP almacenadas en el servidor DNS. En Windows 2003, los servidores y los clientes DHCP pueden registrar y actualizar dinámicamente esta información de los servidores DNS configurados para permitir actualizaciones dinámicas.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.10.1 Protocolo de actualización dinámica

El protocolo de actualización dinámica permite a los equipos cliente actualizar automáticamente sus registros de recursos en un servidor DNS sin necesidad de intervenir el administrador. De forma predeterminada, los equipos con Windows 2000, Windows XP y Windows Server 2003 se configuran para realizar actualizaciones dinámicas cuando también se configuran con una dirección IP estática.

3.10.2 Proceso de actualización dinámica

Cuando un servidor DHCP asigna una dirección IP a un cliente DHCP basado en Windows 2000 ó Windows Server 2003, se produce el siguiente proceso:

1. El cliente inicia un mensaje de solicitud DHCP al servidor DHCP, en el que solicita una dirección IP. Este mensaje incluye el nombre de dominio completo.
2. El servidor DHCP devuelve al cliente un mensaje de confirmación DHCP, en el que se otorga una concesión de dirección IP.
3. El cliente envía al servidor DNS una solicitud de actualización DNS de su propio registro de búsqueda directa, el registro de recursos A (dirección).
4. El servidor DHCP envía actualizaciones para el registro de búsqueda inversa del cliente DHCP, el registro de recursos PTR (puntero). Para realizar esta operación, el servidor DHCP utiliza el nombre de dominio completo que obtuvo en el primer paso.

3.10.3. Actualizaciones dinámicas para clientes con versiones anteriores de Windows

Los equipos cliente que ejecutan versiones anteriores de Windows no admiten actualizaciones dinámicas. Debe configurar el servidor DHCP para que actualice siempre los registros de recursos A y PTR de esos clientes. En tal caso, se produce el proceso siguiente:

1. El cliente inicia un mensaje de solicitud DHCP al servidor DHCP, en el que solicita una dirección IP. A diferencia de los mensajes de solicitud DHCP de los clientes DHCP basados en Windows 2000, la solicitud no incluye un nombre de dominio completo.
2. El servidor devuelve al cliente un mensaje de confirmación DHCP, en el que se otorga una concesión de dirección IP.
3. El servidor DHCP envía al servidor DNS actualizaciones de los registros de recursos A y PTR del cliente.

3.10.4. Configuración del DNS Server para permitir actualizaciones dinámicas

Para configurar un servidor DNS de modo que permita actualizaciones dinámicas, abra el cuadro de diálogo ***Propiedades*** de la zona en el servidor DNS que desee configurar. En la ficha ***General***, en el cuadro de lista ***¿Allow Dynamic updates?***, haga click en ***Yes***. En la tabla siguiente se describen las opciones disponibles para las actualizaciones dinámicas.

No Deshabilita las actualizaciones dinámicas para la zona
Yes Habilita las actualizaciones dinámicas para la zona
Only secure updates Permite las actualizaciones dinámicas seguras de una zona integrada de Active Directory realizadas desde equipos cliente autorizados.

Para obtener más información acerca de DNS:

http://www.microsoft.com/Windows2000/technologies/communications/dns/default.asp

http://support.microsoft.com/default.aspx?scid=kb;en-us;814591

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by ITsitio

http://support.microsoft.com/default.aspx?scid=kb;en-us;323445

http://support.microsoft.com/default.aspx?scid=kb;en-us;323380

http://support.microsoft.com/default.aspx?scid=kb;en-us;323383

http://support.microsoft.com/default.aspx?scid=kb;en-us;323419

http://support.microsoft.com/default.aspx?scid=kb;en-us;324259

http://support.microsoft.com/default.aspx?scid=kb;en-us;324260

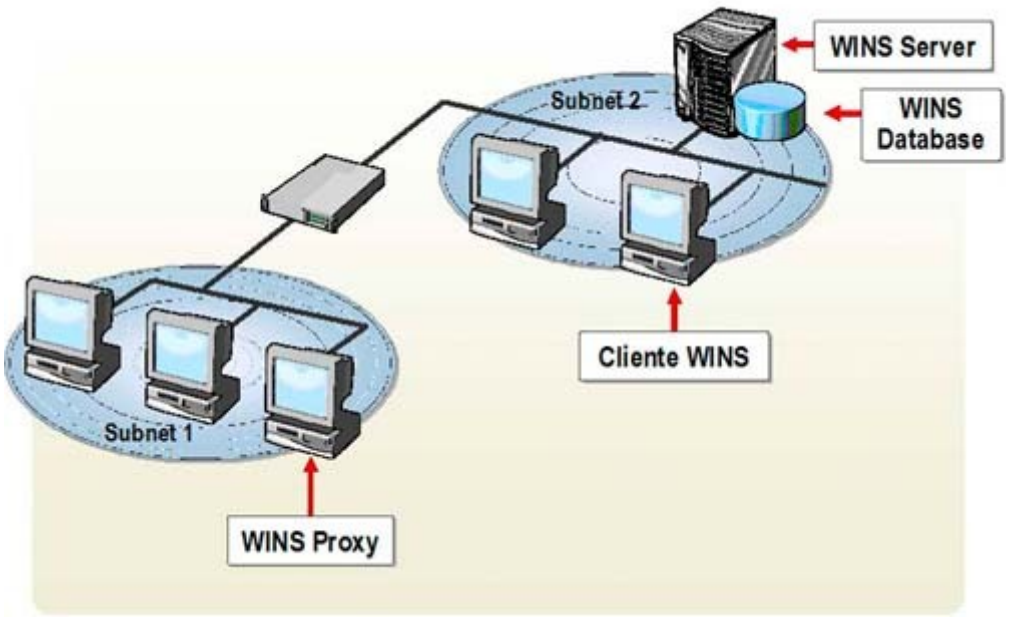
http://support.microsoft.com/default.aspx?scid=kb;en-us;323417

http://support.microsoft.com/default.aspx?scid=kb;en-us;816518

http://support.microsoft.com/default.aspx?scid=kb;en-us;816567

http://support.microsoft.com/default.aspx?scid=kb;en-us;323418

4. Descripción de WINS (Windows Internet Name System)



El método más habitual para resolver nombres NetBIOS remotos y locales es el uso de un servidor de nombres NetBIOS.

Cuando un usuario ejecuta determinados comandos, como ***net use***, o hace que una aplicación NetBIOS interactúe con la red, se inicia el proceso de resolución de nombres NetBIOS. En n la caché de nombres NetBIOS es donde se comprueba si se encuentra la asignación de nombre NetBIOS en dirección IP del host de destino. En caso que el nombre NetBIOS no se encuentre en la caché, el cliente intentará determinar la dirección IP del host de destino mediante otros métodos.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Si el nombre no se puede resolver con la caché, el nombre NetBIOS del host de destino se envía al servidor de nombres NetBIOS configurado para el host de origen. Una vez que el nombre se convierte en una dirección IP, se devuelve al host de origen.

WINS es la implementación de Microsoft de un servidor de nombres NetBIOS.

Para que WINS funcione correctamente en una red, cada cliente debe:

- Registrar su nombre en la base de datos WINS. Al iniciar un cliente, éste registra su nombre en el servidor WINS configurado.
- Renovar el registro a intervalos configurables. Los registros de los clientes son temporales y, por lo tanto, los clientes WINS deben renovar regularmente su nombre o, de lo contrario, su concesión caducará.
- Liberar los nombres de la base de datos al cerrarse. Si el cliente WINS ya no necesita su nombre, por ejemplo cuando se apaga, envía un mensaje para indicar al servidor WINS que lo libere.

Una vez que se ha configurado con WINS como método de resolución de nombres, el cliente también lo usará para llevar a cabo consultas de nombres NetBIOS. Para ello debe realizar las acciones siguientes:

1. Si el cliente no puede resolver el nombre en su caché, envía una consulta de nombre a su servidor WINS principal. Si éste no responde, el cliente enviará la solicitud dos veces más.
2. Si el cliente no recibe una respuesta del servidor WINS principal, vuelve a enviar la solicitud a todos los servidores WINS adicionales, configurados en el cliente. Si un servidor WINS resuelve el nombre, responderá al cliente con la dirección IP del nombre NetBIOS solicitado.
3. En caso que no se reciba ninguna respuesta, el servidor WINS enviará un mensaje indicando que el nombre no se encuentra, y el cliente pasará al siguiente método de resolución de nombres configurado.

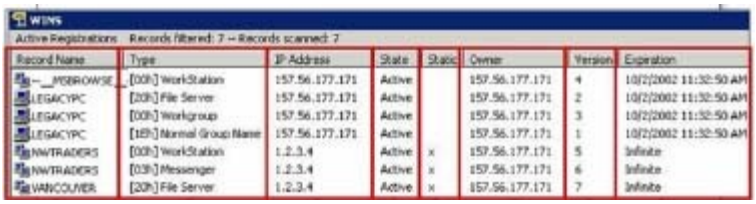
4.1 Práctica 10: Instalación de WINS

Para crear un servidor WINS, instale WINS en un equipo donde se ejecute ***Windows Server 2003***.

Para instalar WINS deberá:

1. Hacer doble click en ***Add / remove programs*** del Panel de control.
2. Hacer click en ***Add / remove Windows components***.
3. Hacer click en Network Services y en Details de la página ***Windows components*** del Asistente para componentes de Windows, en ***Components***.
4. Activar la casilla de verificación ***WINS Service*** En el cuadro de diálogo ***Network Services***, en ***Subcomponents***, y hacer click en ***Ok***.
5. Hacer click en ***Next***.

4.2. Estudio de los registros de la base de datos WINS



La opción WINS de Microsoft Management Console (MMC) permite al usuario ver el contenido de la base de datos WINS y buscar entradas específicas.

Apertura de la base de datos WINS

Para abrir la base de datos WINS deberá:

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

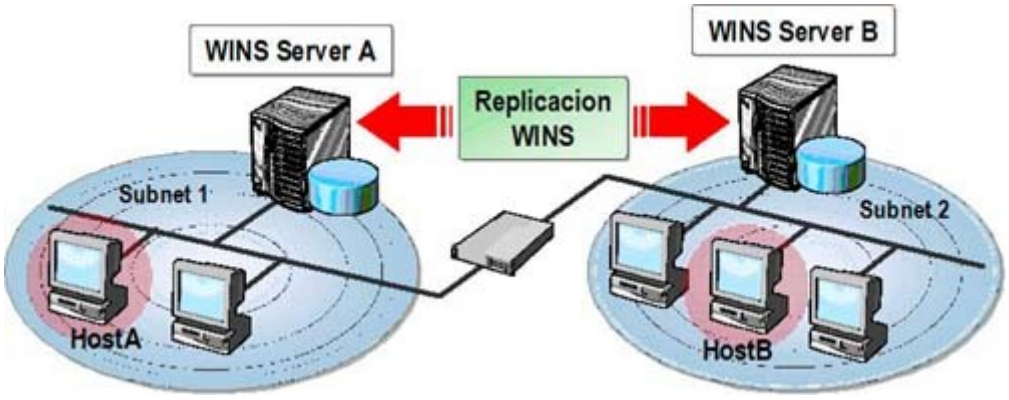
1. Expandir el nombre del servidor en WINS y hacer click en ***Active registries***.
2. Hacer click con el botón secundario del mouse en ***Active registries*** y luego hacer click en ***find by owner***.
3. Hacer click en ***All Owners*** del cuadro de diálogo ***find by owner***, en la ficha ***Owners***, y luego hacer click en ***Find***.

4.2.1. Estudio de la información de registro de WINS

WINS muestra todos los registros de la base de datos y organiza la información de registro de WINS en las columnas siguientes:

- ***Nombre de registro.*** El nombre NetBIOS registrado, que puede ser un nombre único o puede representar a un grupo, un grupo de Internet o un equipo multitarjeta.
- ***Tipo.*** El servicio que registró la entrada, incluido el identificador de tipo hexadecimal.
- ***Dirección IP.*** La dirección IP correspondiente al nombre registrado.
- ***Estado.*** El estado de la entrada de la base de datos, que puede ser Activo, Liberado o Desechado. Si el estado de la entrada es Desechado, ésta ya no estará activa y se quitará de la base de datos.
- ***Propietario.*** El servidor WINS desde que se origina la entrada. Debido a la replicación, no es necesariamente el mismo servidor desde el que se está viendo la base de datos.
- ***Versión.*** Número hexadecimal único, asignado por el servidor WINS durante el registro de nombres. Los asociados del servidor lo utilizan para identificar nuevos registros durante la replicación.
- ***Caducidad.*** Muestra la fecha de caducidad de la entrada. Cuando un replicado se almacena en la base de datos, los datos de caducidad correspondientes se establecen de acuerdo con la hora del servidor WINS de recepción, además del intervalo de renovación establecido en el cliente.

4.3. Replicación de WINS



Aunque un servidor WINS puede admitir más de 5.000 clientes en condiciones normales de carga de trabajo, puede instalar también un segundo servidor para proporcionar tolerancia a errores en la resolución de nombres NetBIOS. Dicho servidor permitirá, al mismo tiempo, localizar el tráfico de resolución. De esta forma, si se produce un error en uno de los servidores WINS, el otro servidor continuará realizando la resolución de nombres NetBIOS en la red.

Cada servidor WINS de una red mantiene su propia base de datos WINS. Por lo tanto, si hay varios servidores WINS en la red, deberán configurarse para replicar los registros de su base de datos en el resto de los servidores WINS. La replicación de bases de datos WINS garantiza que un cliente WINS configurado para usar un servidor WINS distinto, pueda resolver nombres registrados con un servidor WINS.

Por ejemplo:

- El host A de la subred 1 se registra con el servidor WINS A de la subred 1.
- El host B de la subred 2 se registra con el servidor WINS B de la subred 2.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

- Cuando se produce una replicación de WINS, cada servidor WINS actualiza su base de datos con la nueva entrada procedente de la base de datos del otro servidor.

Como resultado de la replicación, ambos servidores WINS disponen de información acerca de ambos hosts, y los hosts A y B pueden resolver mutuamente sus nombres si se ponen en contacto con su servidor WINS local.

Para que se produzca la replicación, cada servidor WINS deberá configurarse con un asociado de replicación, como mínimo. Al configurar un asociado de replicación para un servidor WINS, puede especificarlo como asociado de extracción, como asociado de inserción o como asociado de extracción e inserción para el proceso de replicación.

4.3.1 ¿Cómo funciona la replicación Push?

4.3.1.1. Definición

La replicación ***Push*** es el proceso de copia de los registros actualizados desde un WINS Server a otros, siempre que el WINS Server que contenga datos actualizados, alcance un valor especificado de cambios.

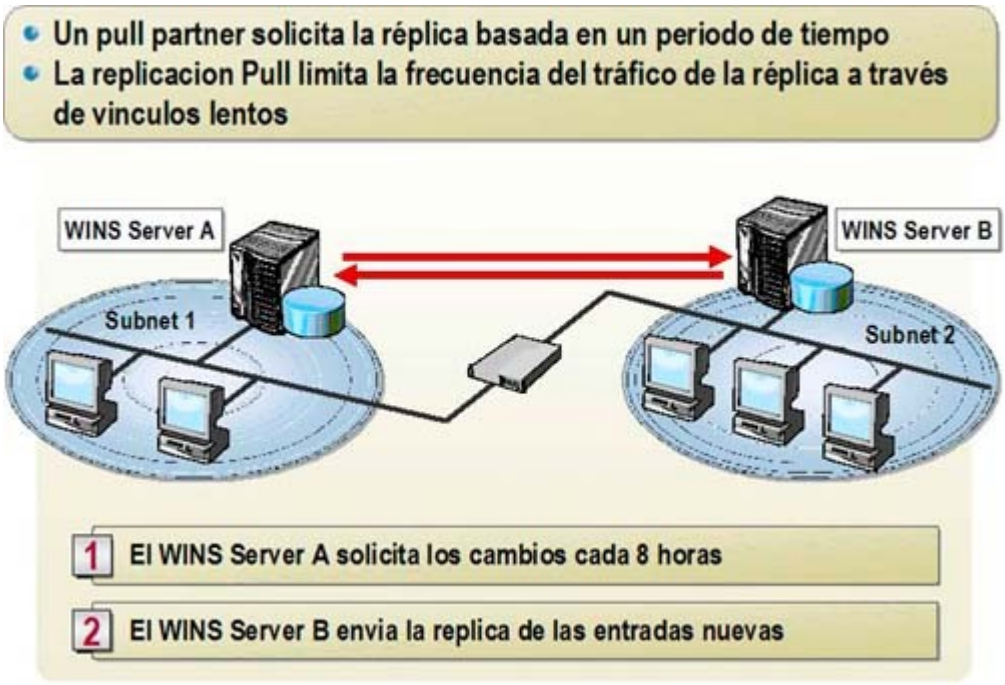
El proceso de replicación Push funciona de la siguiente forma:

1. El Push Partner notifica a sus Replication Partners, siempre que el número de cambios a su base de datos del WINS pase un valor específico configurable. Por ejemplo, Usted puede configurar el Push Partner para notificar a los Replication Partners cuando ocurran 50 cambios en la base.
2. Cuando los Replication Partners respondan a la notificación con un pedido de réplica, el Push Partner envía la réplica de las entradas nuevas en la base.

4.3.2 ¿Cómo funciona una replicación Pull?

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by



4.3.2.1. Definición

La replicación ***Pull*** es el proceso de copia de los registros actualizados desde un WINS Server a otros WINS Servers, en intervalos específicos de tiempo.

El proceso de replicación Pull funciona de la siguiente forma:

1. El Pull Partner solicita los cambios en la base de WINS en intervalos de tiempo. Por ejemplo, Usted puede configurar un Pull Partner para solicitar los cambios cada 8 horas.
2. Los Replication Partners responden enviando las entradas nuevas de la base.

También existe la posibilidad de configurar Replications Partners de modo Push/Pull. Esto le asegura que bajo determinada cantidad de cambios, se produzca la replicación en intervalos de tiempo.

4.4. Práctica 11: ¿Cómo configurar una replicación WINS?

Para poder hacer esta práctica Usted necesitará dos instalaciones de Windows Server 2003 con el servicio de WINS instalado.

Por default, los WINS Replication Partners son configurados como Push/Pull Partners. Para modificar esta configuración y satisfacer las necesidades de su red, Usted puede especificar los parámetros Push y Pull para cada Replication Partner.

Para configurar una replicación WINS deberá:

1. Seleccionar, en la consola WINS, el WINS Server al que quiere agregar un Replication Partner, y hacer click en ***Replication Partners***.
2. Hacer click en ***New Replication Partner*** del menú ***Action***,
3. Ingresar, en el campo ***WINS Server***, el nombre o la IP del WINS Server a agregar como Replication Partner. (Segunda Computadora)
4. Hacer click en ***OK***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Para modificar el tipo de Replication Partner deberá:

1. Expandir el WINS Server en la consola WINS.
2. Hacer click en ***Replication Partners*** de la consola WINS.
3. Hacer click derecho en el server apropriado del cuadro de detalles, y luego hacer click en ***Properties***
4. Seleccionar una de las siguientes opciones en el cuadro Server ***Properties***, en ***Advanced***, en el campo: ***Replication partner type***:
   - ***Push.***
   - ***Pull.***
   - ***Push/Pull.***
5. Hacer click en ***OK*** del cuadro ***Server Properties***.
6. Cerrar la consola WINS.

Para obtener más información acerca de WINS:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323429

4.5. Mantenimiento

4.5.1. Backup

Usted debe realizar tareas de mantenimiento en períodos de tiempo específico. Para ayudarle en esta tarea, el WINS Server puede ser configurado para realizar los backups automáticamente. Tenga en cuenta que todos los software de backup no realizan esta tarea ya que la base de datos es un archivo con privilegios exclusivos del sistema operativo, siempre que el servicio esté iniciado.

Para especificar el directorio de backup de WINS deberá:

1. Hacer click derecho sobre el WINS Server de la consola WINS, y después hacer click en ***Properties***.
2. Ingresar el directorio donde quiere realizar los backups del WINS Server, en ***General*** en el campo ***Default backup path***.

Nota: El WINS Server realizará un backup automáticamente cada 24 horas.

4.5.2. Compactar la base de datos

Para realizar las operaciones de reparación y/o compactación debe utilizar la herramienta apropiada: la base de WINS, que es un archivo que se encuentra en \Windows\system32\Wins y su nombre es Wins.mdb. La herramienta que usted debe utilizar es jetpack, y el comando es:

jetpack %Systemroot%\System32\Wins\Wins.mdb Temp.mdb

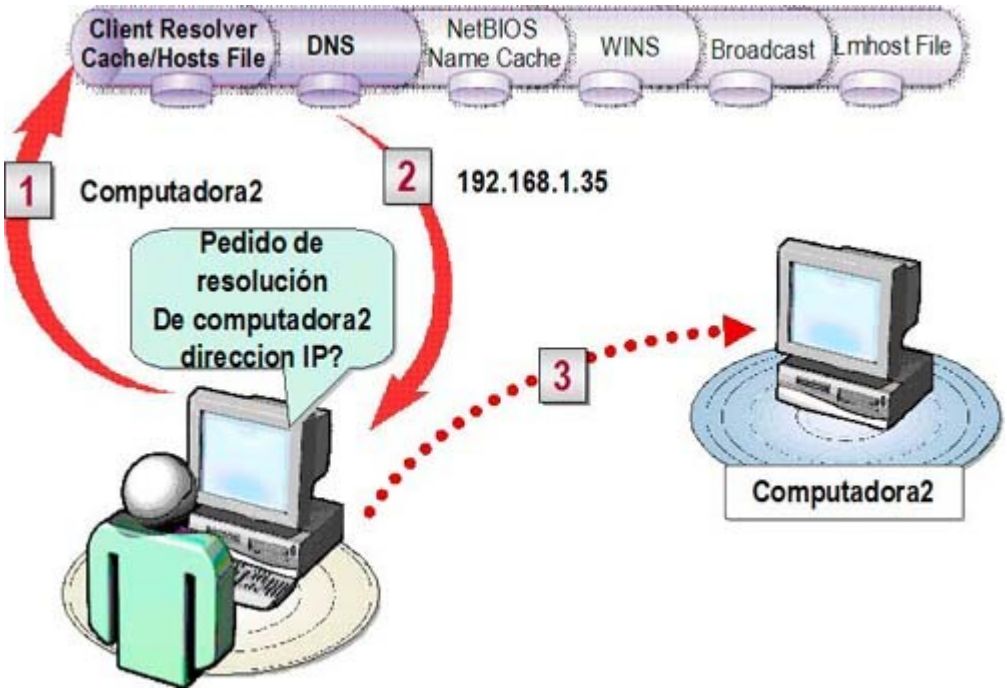
Donde %systemroot% es el directorio de instalación del sistema operativo y temp,mdb es una base temporal.
Luego debe copiar la base temporal con el nombre Wins.mdb y eliminar la base anterior. Recuerde que para realizar esta tarea debe estar detenido el servicio de WINS Server.

4.6. Procesos de resolución de nombres e integración WINS / DNS

4.6.1. Resolución de nombres de host

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio



El proceso de resolución de nombres de HOST en un cliente cumple con el siguiente diagrama:

1. El cliente verifica si ya obtuvo la resolución en otra oportunidad. De ser así la resolución se encuentra en el DNS caché local del cliente y finaliza el proceso. Si no obtiene la resolución, sigue al paso siguiente.
2. El cliente realiza una query al DNS primario. Si el DNS resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
3. El cliente verifica si ya obtuvo la resolución en otra oportunidad. De ser así, la resolución se encuentra en el NetBIOS caché local del cliente y finaliza el proceso. Si no obtiene la resolución, sigue al paso siguiente.
4. El cliente realiza una query al WINS primario. Si el WINS resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
5. Si hasta el momento no pudo resolver el nombre, el cliente realiza un Broadcast local. Si resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
6. Por último tendrá que consultar el archivo local HOST que se encuentra en systemroot\ system32\drivers\etc. Este archivo es una base estática de resolución; no tiene extensión y tampoco se actualiza. Si este último proceso no es exitoso, el cliente no logra la resolución.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Ejemplo de archivo HOST

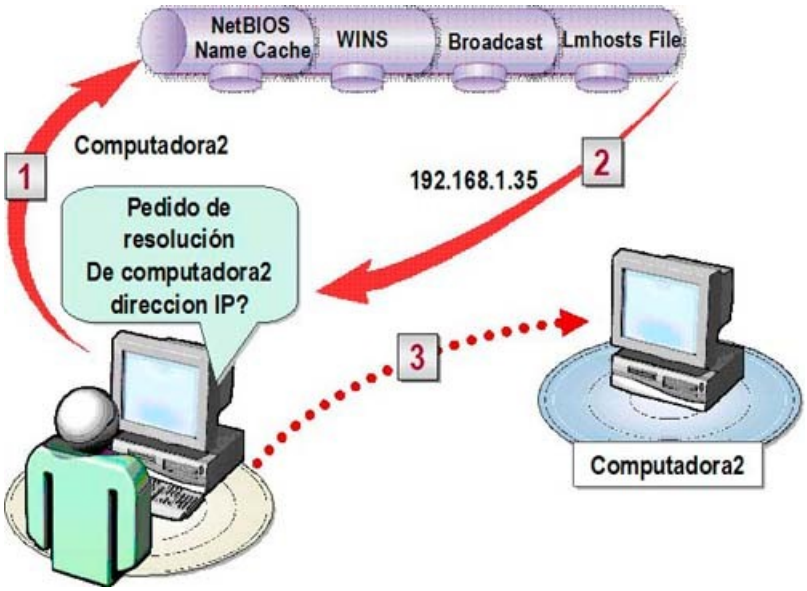
```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

4.6.2. Resolución de nombres NetBIOS

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by



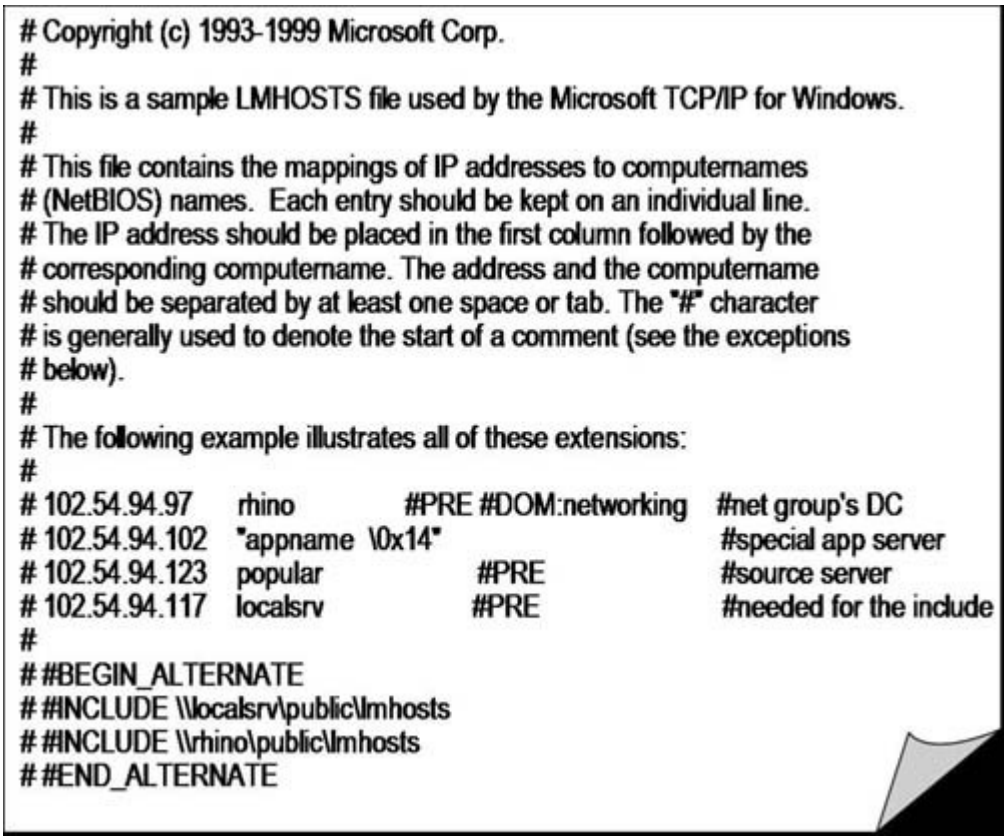
El proceso de resolución de nombres de NetBIOS en un cliente cumple con el siguiente diagrama:

1. El cliente verifica si ya obtuvo la resolución en otra oportunidad. De ser así, la resolución se encuentra en el NetBIOS caché local del cliente y finaliza el proceso. Si no obtiene la resolución, sigue al paso siguiente.
2. El cliente realiza una query al WINS primario. Si el WINS resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
3. Si hasta el momento no pudo resolver el nombre, el cliente realiza un Broadcast local. Si resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
4. Por último tendrá que consultar el archivo local LMHOST que se encuentra en systemroot\system32\drivers\etc. Este archivo es una base estática de resolución; no tiene extensión y tampoco se actualiza. Si este último proceso no es exitoso, el cliente no logrará la resolución.

Ejemplo de Archivo LMHOST

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

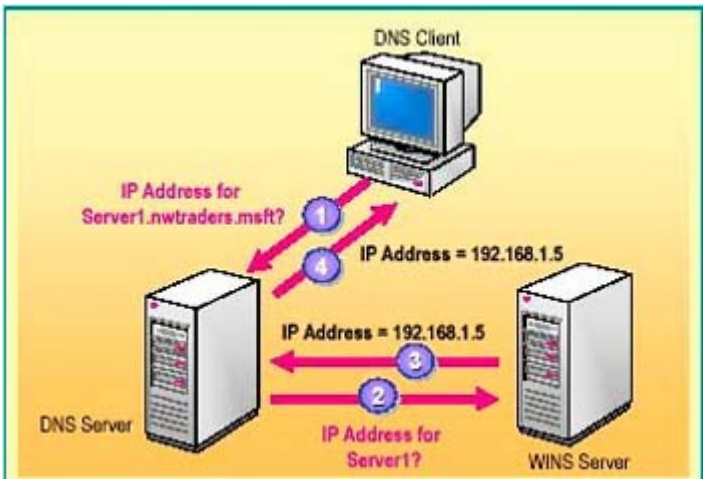


```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino          #PRE #DOM:networking   #net group's DC
# 102.54.94.102    "appname  \0x14"                      #special app server
# 102.54.94.123    popular              #PRE             #source server
# 102.54.94.117    localsrv             #PRE             #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
```


© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

4.6.3. Introducción a la integración WINS y DNS



El integrar WINS con DNS habilita a los clientes a usar exclusivamente DNS para la resolución de nombres. Los clientes podrán acceder a los datos de WINS a través del DNS server. Sin embargo, el DNS Server no puede localizar recursos sin realizar una query a WINS. En Windows Server 2003, Usted puede configurar integración entre WINS y DNS para habilitar a clientes no-WINS para resolver nombres NetBIOS, usando un DNS Server.

Usted puede configurar DNS integrado con WINS Servers.

Para configurar una zona DNS para uso de WINS lookup deberá:

1. Abrir DNS en el menú ***Administrative Tools***.
2. Expandir, en la consola DNS, el server donde está la zona a configurar, expandir ***Forward Lookup Zones***, y luego hacer click en la zona.
3. Hacer click derecho en la zona, y luego en ***Properties***.
4. Seleccionar el cuadro Use ***WINS forward lookup***, del cuadro ***Properties***, en ***WINS***.
5. Ingresar la dirección IP del WINS Server, del cuadro ***IP address***, y luego hacer click en ***Add***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by